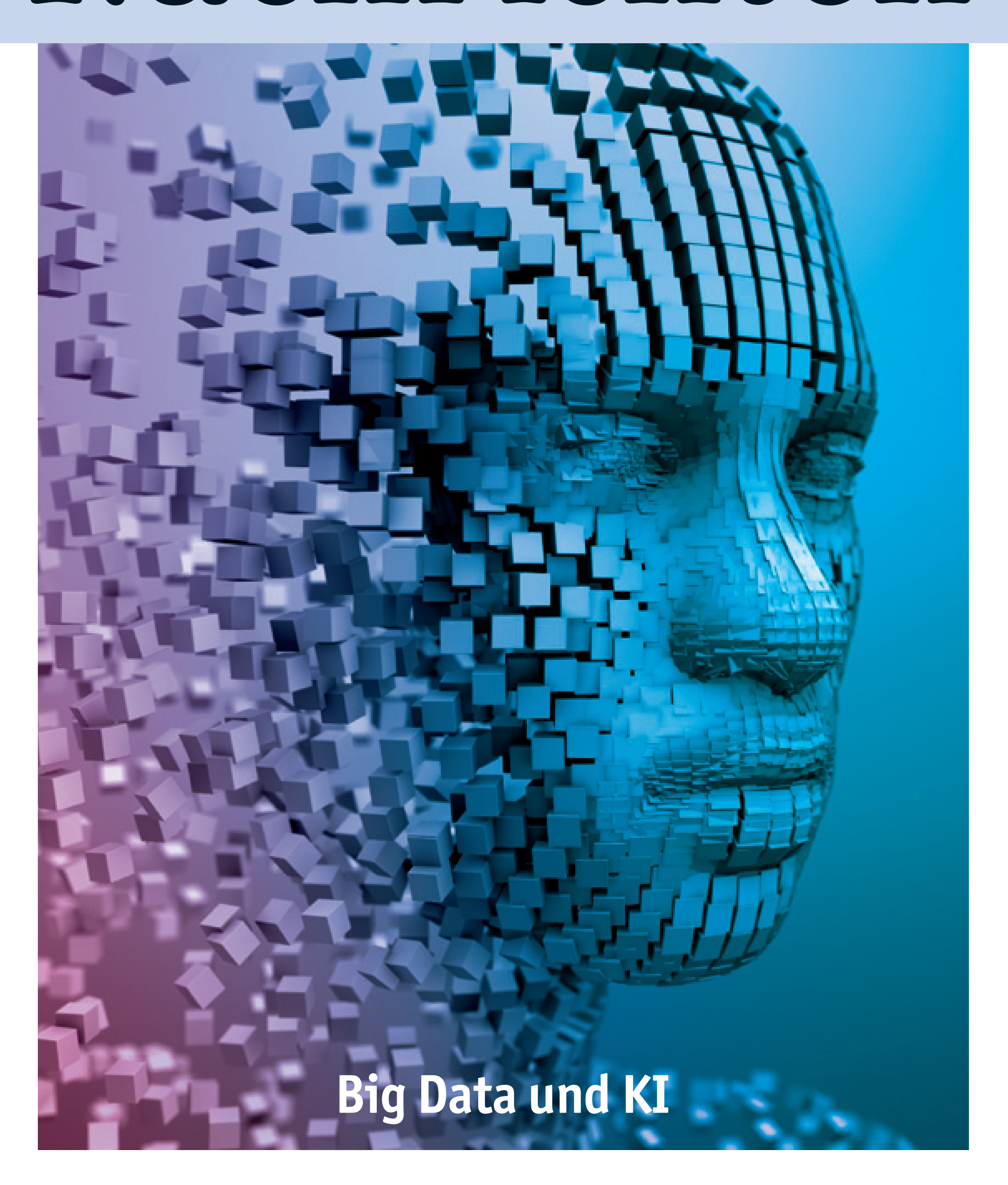
3/2018

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

41. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Die große Big-Data-Illusion ■ Algorithmen sind Gesetz – Code is Law ■ Die verfassungsrechtliche Dimension der Algorithmenkontrolle ■ Algorithmen-basierte Entscheidungsprozesse und Verbraucherschutz ■ Datenschutzaufsicht und Politik ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Mittwoch, 17. Oktober 2018 –
Donnerstag, 18. Oktober 2018
ABIDA Gutachtertagung – Big Data: Intelligente Datenanalyse für die Datenökonomie
Berlin
http://www.abida.de/de/blog-item/guterachterfachtagung-big-data-intelligente-datenanalyse-für-die-datenökonomie

Samstag, 20. Oktober 2018
DVD-Vorstandssitzung
Bonn

Sonntag, 21. Oktober 2018
DVD-Mitgliederversammlung
Bonn

Dienstag, 23. Oktober 2018
E-Privacy-Verordnung – was kommt auf uns zu?
Berlin
https://www.stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/news/eprivacy-aktueller-stand-und-ausblick-in-kooperation-mit-dem-dihk/

Donnerstag, 01. November 2018
Redaktionsschluss DANA 4/2018

Donnerstag, 22. November 2018
Dateneigentum und Datenhandel kompakt – Wem unsere Daten künftig gehören (können)
Berlin
https://www.esv.info/lp/esv-akademie/datenhandel

DANA
Datenschutz Nachrichten
ISSN 0137-7767
41. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, iStock, Pixabay

Editorial

Die Schlacht um die DSGVO ist vorläufig ausgefochten; das Hauen und Stechen um die ePrivacy-Verordnung kommt nicht so richtig voran. Dass solche Zeiten nicht ohne Auseinandersetzungen bleiben, dafür sorgt die technische Entwicklung. Diese ist geprägt vom Siegeszug von Big Data und – so heißt es zumindest – der „künstlichen Intelligenz“. Tatsächlich kommt kaum noch ein modernes technisches Gerät ohne komplexe Algorithmen aus, mit denen dessen Anwendung erleichtert, verbessert werden soll. In unseren Netzgeräten, vom PC über das Tablet bis zum Smart Phone stecken hochgradig komplexe Algorithmen, die bestimmen, was wir sehen, was wir lesen, mit dem wir kommunizieren, was wir spielen, für was wir uns interessieren. Auch viele Geräte, denen wir die Vernetzung gar nicht ansehen, z. B. unsere Autos, nehmen an diesem Trend teil. Dass damit an Selbstbestimmung für uns verloren geht, ist uns individuell kaum bewusst. Es ist fast ein Treppenwitz, wären die Folgen nicht global so gravierend, dass die Algorithmen des Silicon Valley dazu beigetragen haben, dass ein Trump gewählt und für einen Brexit gestimmt worden ist: Zwei Entscheidungen, die schwerlich mit dem global-libertären Selbstverständnis der meisten Algorithmen-Macher im Südwesten der USA in Einklang stehen.

Die Algorithmen entwickeln eine eigene Dynamik, keine Eigendynamik: Sie werden eingesetzt zur Beherrschung der Welt und deren Bewohner. Wie dies bewusst und gezielt geschieht, exerziert uns die Volksrepublik China vor. In einer solchen digital gesteuerten Überwachungsgesellschaft wollen wir nicht leben. Auf der Tagesordnung steht daher zwangsläufig die Algorithmenkontrolle, der sich das vorliegende Heft schwerpunktmäßig widmet: Sarah Spiekermann zeigt uns auf, wie digitale und reale Welt auseinanderdriften. Dann haben wir einen 18 Jahre alten klassischen Text von Lawrence Lessig übersetzt, der visionär darlegt, wie der Algorithmus zum Gesetz wird. Lina Ehrig und Miika Blinn vom Verbraucherzentrale Bundesverband (vzbv) thematisieren die verbraucherpolitischen Herausforderungen. Ich selbst nehme eine verfassungsrechtliche Bewertung vor und mache einen ersten praktischen Vorschlag zur Algorithmuskontrolle.

Ergänzt wird das Heft durch Klaus-Jürgen Roth, der das Verhältnis der Politik in Schleswig-Holstein zur Regulierung der Datenschutzkontrolle nachvollzieht, sowie wieder durch viele aktuelle Meldungen aus dem In- und Ausland, von der Technik, aus der Rechtsprechung und zur Literatur. Es ist also wieder Spannendes für die spätsommerliche Lektüre geboten. Viel Spaß und Erkenntnisgewinn dabei.

Thilo Weichert

Autorinnen und Autoren dieser Ausgabe:

Miika Blinn
Referent Digitales und Medien, Verbraucherzentrale Bundesverband e. V. (vzbv)
digitales@vzbv.de

Lina Ehrig
Leiterin Team Digitales und Medien Geschäftsbereich Verbraucherpolitik im vzbv
digitales@vzbv.de

Prof. Lawrence Lessig
Professor für Unternehmensrecht an der Harvard Law School, Berkman Klein Center

Klaus-Jürgen Roth
dvd@datenschutzverein.de

Prof. Sarah Spiekermann
Leiterin des Instituts für BWL und Wirtschaftsinformatik an der Wirtschaftsuniversität Wien

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Sarah Spiekermann

Die große Big-Data-Illusion

Konzerne, die in großem Stil Daten erheben und mit ihnen handeln, behaupten, sie wüssten alles. Dabei verzerren sie das Bild des Menschen und von der Welt. Ihr falsches Spiel muss ein Ende haben.

Ich denke, dass wir uns – politisch, wirtschaftlich und persönlich – schnellstmöglich darüber Gedanken machen müssen, wie wir dafür Sorge tragen, dass Digitalisierung auch in Zukunft unserem menschlichen und unternehmerischen Wohlbefinden dient und nicht sehr bald ihre eigenen (Vorteils-) Kinder frisst.

Digitalisierung war einmal gut. In den achtziger und neunziger Jahren konnten ungeheure wirtschaftliche und private Vorteile durch sie geschaffen werden. Das Netz war ein ökonomisches Integrationsprojekt, ein Demokratieprojekt und ein Projekt, das uns Zugang zu Wissen gegeben hat. Aber seit digitale Geräte breitbandig vernetzt sind und angefangen haben, ein Eigenleben zu entwickeln, was uns abhängig macht und dauerhaft überwacht, geht es bergab. In meiner Forschung interessiere ich mich im Moment dafür, was diesen „Knackpunkt" Richtung Abgrund ausmacht. Was dazu gehört, nenne ich die „Big-Data-Illusion".

Wir sehen Filme und Serien wie „Ex Machina", „Westworld" oder „Humans", die hochintelligente Humanoide (Roboter) vorstellen. Große Museen organisieren transhumanistische Ausstellungen zur dunklen Zukunft der Menschen als Cyborgs. In Saudi-Arabien erhielt eine Roboterfrau namens Sophia sogar die Staatsbürgerschaft und hielt eine völlig absurde Rede, der UN-Mitarbeiter zu huldigen hatten wie einem goldenen Kalb. Big Data, so wird uns erzählt, bringt auf magische Weise superintelligente Wesen in die Welt, die die Menschheit retten werden.

Aber ganz ehrlich. Wie soll Big Data jemals auch nur ansatzweise intelligent im menschlichen Sinne sein? Ich will großen Datenmengen nicht absprechen, dass sie neben einer Menge Rauschen Muster erkennen, die uns als Menschen entgehen und die durchaus interessant, ja wichtig sein können. Die KI hat ihren eigenen Platz in der Intelligenzgeschichte. Aber das, was für uns Menschen von Bedeutung ist, im Privatleben, in der Firma, in der Politik, das kann und wird sie niemals erfassen.

Sympathie, Schönheit, Zauber, Ehrfurcht, Frömmigkeit, Neugierde, Sorge. Es geht um Werte, die sich mit unseren Erinnerungen und externen Stimuli durchmischen, um das zu generieren, was für uns in der Gegenwart den Raum des Bewusstsein bildet, wobei dieser Raum gleichermaßen von Vergangenheit und Zukunft bestimmt ist wie von relevantem Entferntem und bedeutsamem Nahem. All das jedoch ist unsichtbar. Es ist nicht messbar, nicht beobachtbar, nicht fassbar, nicht extrapolierbar. Kein digitaler Sensor dieser Welt kann dieses Unsichtbare messen. Maschinen haben keinerlei Einblick in das, was für einen Menschen an Ort und Stelle von Bedeutung ist. Wenn dem aber so ist, wie sollen dann all diese Roboterfiktionen jemals wahr werden?

Worin Maschinen wirklich gut sind, ist Secondhand-Daten zu erfassen. Facebook kann sofort auf Fotos erkennen, ob jemand lacht und darauf schließen, dass derjenige wohl glücklich gewesen sein muss. Facebook weiß, ob die Paare auf den Fotos verheiratet sind, weil es vielleicht vom Meldeamt Informationen erworben hat, oder weil die Paare das selbst auf der Plattform angegeben haben. Aufgrund des Geotaggings könnte Facebook bei einem Foto vom Vatikan glauben, dass derjenige, der das Foto hochgeladen hat, tatsächlich dort war. Smartphone-Daten können diese Informationen noch viel genauer erfassen. Es kann genau nachvollzogen werden, an welchen Orten jemand nacheinander war, welcher Art diese Orte sind. Mobilfunkgeräte wissen, wie groß eine Menschenmenge ist oder ob es dem Besitzer des Geräts gutgeht, denn die Bewegungssensoren bekommen mit, wie schnell oder langsam sich jemand im Vergleich zu anderen Tagen bewegt. Emotionale Worte und Emojis in Messages und Mails zeigen an, wie gut jemand gerade gelaunt ist. Aus solchen Daten können Maschinen eine Menge über unser Leben und unsere Persönlichkeit schließen.

Es gibt nur einen Haken. Ich bin nicht auf Facebook und mein Mann auch nicht und keiner unserer engen Freunde. Fotos, auf denen nicht gelächelt wird, stellt ohnehin kaum jemand online. Ständig posten Leute Fotos von Plätzen, an denen sie nie waren und entnehmen schöne Bilder aus Fotogalerien. Man überlegt sich zweimal, was man online sagt. Das Mobiltelefon könnte man durchaus zu Hause gelassen haben. Dann denken die Betreiber, Hersteller und App-Provider, die auf die Smartphone-Daten in Echtzeit zugreifen, dass man vielleicht depressiv im Bett liegt und niemandem mehr schreibt, wo man in Wirklichkeit fröhlich woanders unterwegs war.

Was heißt das? Der Secondhand-Eindruck von uns, der heute mit dem Begriff Big Data beschrieben wird, ist zwar umfassend, aber er zeichnet ein Bild von uns, das nicht unbedingt mit unserer Realität übereinstimmt. Während uns die Schöne-neue-Welt-Spezialisten aus dem Silicon Valley glauben lassen wollen, sie würden virtuelle Spiegelwelten schaffen, lassen uns klügere Leute wie Jaron Lanier wissen, was sie davon halten: „Die tiefe Bedeutung des menschlichen Daseins wird reduziert auf eine Illusion von Bits."

In der Tat wissen die Leute, die heute Big Data sammeln, verwalten und nutzen, nur zu gut um dieses Defizit. Deswegen kommen heute noch 95 Prozent der Werbebotschaften zum falschen Zeitpunkt. Jeder, der mit KI und Daten gearbeitet hat, weiß dass die Daten nicht vollständig, dass sie oft falsch, dass sie selektiv sind und dass sie über

Kontexte hinweg verbunden und verfremdet werden. Künstliche Intelligenzen machen die absurdesten Klassifikationsfehler. Wenn man mit diesen Fehlern weiterrechnet, entsteht noch mehr Unsinn. Dabei stehen die Datensammler unter Druck, denn ihre absurd hohen Börsennotationen hängen davon ab, dass die ganze Welt an Big Data als „Öl" der Digitalökonomie glaubt. So haben die Firmen mit der Jagd nach noch mehr Daten begonnen. Sie sind auf der Suche nach dem Unsichtbaren, dem nicht messbaren, dem wahren Kern des menschlichen Bewusstseins.

Eine Strategie ist, uns mit noch mehr Technologie einzudecken, uns zu „envelopen". Umfangen sollen wir sein in Smart Homes, von Smart Clothing, Smart Glases, Smart Chips und vielleicht sogar bald Chips unter der Haut haben, die ein Cyborg-Leben für uns einläuten. Doch während wir lustig ignorant mit diesem ganzen IT-Zeugs spielen, entstehen da draußen gigantische Datenbanken über uns voller Fehler und Einseitigkeiten.

Nahmen wir mal eine Firma wie Acxiom, die laut ihres Geschäftsberichts 2016 Daten über siebenhundert Millionen Personen hat und verspricht, zu den Menschen fünftausend Datenpunkte liefern zu können, inklusive Daten zu nahezu jedem deutschen Haushalt. Die Firma Oracle sagt im Januar 2017, sie könne über ihre Oracle-Bluekai-Datenplattform auf zwei Milliarden Konsumentenprofile weltweit zugreifen mit angeblich dreißigtausend Attributen pro Person, die sie von tausendfünfhundert Datenlieferanten bekommt.

Acxiom und Oracle sind nur die größeren von mehr als tausend Firmen, die alle von dem Versprechen leben, dass unsere Daten ihnen Einsicht in das Unsichtbare geben: unsere Werte, unsere Bedürfnisse und unsere Wünsche. Diese Firmen können nicht nur vom Werbegeschäft leben, wenn jeder Mensch heute 3.000 Werbebotschaften am Tag sieht und sich die Leute aufgrund der Informationsflut heute an achtzig Prozent weniger Werbungen erinnern als noch vor ein paar Jahren.

Wovon leben diese Firmen also? Sie leben von einer Unzahl von Anwendungsfeldern, in denen Secondhand-Daten heute als „gut genug" akzeptiert werden und teilweise auch sind. Sie sind in jedem Fall gut genug, um unsere Freiheit und Demokratie zu untergraben, indem sie Facebook helfen, arabische Frühlinge zu organisieren, amerikanische Präsidenten zur Wahl zu verhelfen und Europa durch den Brexit durcheinanderzubringen. Sie werden als gut genug angesehen, um unser Wohlbefinden zu untergraben, weil Banken unsere Kreditwürdigkeit darauf abstellen können, unsere Versicherungsraten anpassen und unsere Flugpreise erhöhen. Sie können herangezogen werden, um Bewerber zu prüfen und damit über die Zukunft von Menschen zu entscheiden.

Sie werden als gut genug angesehen, um Softwareassistenten wie Alexa zu trainieren, die dann unsere Kinder erziehen. Und immer mehr Länder ziehen sie heran, um Polizeieinsätze zu planen und für Bürger – wie in China – individuelle Vertrauensscores zu errechnen. Immer mehr Menschen, Politiker, Sicherheitsbehörden, Journalisten stützen heute ihre Entscheidungen auf ihre eigenen Filter-Bubbles und Echo-Chambers, die auf den Secondhand-Daten aufgebaut sind und die ihnen aus der scheinbar „objektiven" Datenwelt zugespielt werden.

Das Resultat sind politische Konflikte, in denen jeder nur noch seine eigene Wahrheit kennt und der öffentliche Raum als Grundlage jeder Demokratie zerstört ist. So untergräbt eine gigantische Big-Data-Illusion unsere Werte. Es wird Zeit, dass diese Blase endlich platzt, wir die Big-Data-Illusion und ihre Artefakte hinterfragen und endlich wieder Realismus Einzug hält.

Der Text basiert auf Sarah Spiekermanns Laudatio, die sie anlässlich der Verleihung der BigBrotherAwards 2018 in Bielefeld gehalten hat (DANA 2/2018, 94). Eine Erstveröffentlichung dieses Textes erfolgte in der Frankfurter Allgemeinen Zeitung vom 25.04.2018 S. 13.

Lawrence Lessig, übersetzt von Thilo Weichert

Algorithmen sind Gesetz – Code is Law

Über die Freiheit im digitalen Raum

Jedes Zeitalter entwickelt seine eigenen potenziellen Ordnungskräfte und seine Freiheitsbedrohungen. Die Gründungsväter der USA befürchteten eine mit neuer Macht ausgestattete föderale Regierung und erließen die Verfassung als Antwort auf diese Angst. John Stuart Mill befürchtete die Festschreibung der im England des 19. Jahrhunderts bestehenden sozialen Normen; sein Buch „On Liberty" richtete sich gegen diese Festschreibungen. Viele fortschrittliche Menschen befürchteten im 20. Jahrhundert die Ungerechtigkeiten des Marktes. Als Antwort darauf wurden die Marktregulierung und die diese flankierenden sozialen Sicherheitsnetze etabliert.

Unser Zeitalter ist das des Cyberspace, des digitalen Raums. Auch dieser hat eine Ordnungskraft. Auch diese Kraft bedroht unsere Freiheit. Da wir aber so von der Idee gefangen sind, dass Freiheit „Freiheit von der Regierung" bedeutet, erkennen wir nicht die Ordnungskraft dieses neuen Raums. Und deshalb erkennen wir auch nicht die Bedrohung für unsere Freiheit, die diese Kraft darstellt.

Diese Ordnungskraft sind Algorithmen, ist der Computercode – die Soft- und die Hardware, die den digitalen Raum zu dem machen, was er ist. Dieser Code – bzw. die informationstechnische Architektur – legt die Bedingungen fest, unter welchen das Leben im digitalen Raum stattfindet und erlebt wird. Er bestimmt, wie leicht es ist, Privatheit zu schützen, und wie leicht es ist, Meinungsäußerungen zu zensieren. Er bestimmt, ob Informationszugänge generell oder nur eingeschränkt bestehen. Er hat Einfluss darauf, wer was sieht und was kontrolliert wird. Dies geschieht in Erscheinungsformen, die man nicht sieht, solange man nicht die Formen dieses Codes zu verstehen beginnt, des Codes, der den digitalen Raum ordnet.

Diese Ordnung unterliegt einem Wandel. Der Code des digitalen Raums verändert sich. Und so wie sich dieser Code verändert, ändert sich auch der Charakter des digitalen Raums. Dieser Raum wird aus einem Raum, der Anonymität, freie Meinung und individuelle Kontrolle schützt, zu einem Raum, der Anonymität schwieriger, Meinungsäußerung weniger frei und individuelle Kontrolle zu einem nur einzelnen Experten zugänglichen Bereich macht.

Mein Ziel ist es, in diesem kurzen Text eine Gefühl für diese Regulierung zu geben und dafür, wie sich diese verändert. Wenn wir nicht verstehen, wie der digitale Raum Werte unserer Verfassungstradition integriert oder verdrängt, werden wir die Kontrolle über diese Werte verlieren. Das Gesetz im digitalen Raum – die Algorithmen – werden sie verdrängen.

Die Regulierungen durch Algorithmen

Der grundlegende Code des Internet implementiert einen Satz von Protokollen, genannt TCP/IP. Diese Protokolle ermöglichen den Datenaustausch zwischen miteinander verbundenen Netzwerken. Dieser Austausch erfolgt, ohne dass die Netzwerke den Dateninhalt kennen und ohne eine wahre Vorstellung davon zu haben, wer im realen Leben Absender eines speziellen Datenbits ist. Der Code ist neutral gegenüber den Daten und unwissend bezüglich dem Nutzer.

Dieses Charakteristikum von TCP/IP hat Konsequenzen für die Regulierbarkeit des Verhaltens im Internet. Es erschwert die Regulierung von Verhalten. In dem Maße, in dem es schwierig ist zu klären, wer die handelnden Personen sind, wird es schwieriger, Verhalten zu einem spezifischen Individuum zurückzuverfolgen. Und in dem Maße, in dem es schwierig ist zu klären, welche Daten gesendet werden, ist es schwieriger, die Nutzung von besonderen Datenarten zu regulieren. Diese Architekturmerkmale des Internet haben zur Folge, dass Regierungen sich in ihrer Möglichkeit gewissermaßen behindert sehen, Verhalten im Netz zu regulieren.

In bestimmten Zusammenhängen hat diese Unregulierbarkeit für bestimmte Personen einen Wert. Dieses Merkmal des Netzes schützt die freie Meinungsäußerung. Es schreibt den ersten Verfassungszusatz der US-Verfassung in der Architektur des digitalen Raums fest, weil er es Regierungen oder mächtigen Institutionen relativ schwierig macht zu kontrollieren, wer was wann sagt. Informationen von Bosnien oder Osttimor können frei in die Welt gelangen, weil das Netz es den Regierungen in jenen Staaten schwer macht zu kontrollieren, wie Informationen fließen. Das Netz erschwert dies aufgrund seiner Architektur. In anderen Zusammenhängen ist diese Unregulierbarkeit mit einer anderen Perspektive kein Vorteil – etwa wenn die deutsche Regierung mit Nazisprüchen konfrontiert wird oder die US-Regierung mit Kinderpornografie. Die Architektur verhindert dann Ordnung. Unregulierbarkeit kann in solchen Zusammenhängen als schädlich angesehen werden.

Dies gilt nicht nur für Nazisprüche und Kinderpornografie. Die wichtigen Regulierungszusammenhänge werden in Zukunft mit dem Internet-Handel zu tun haben: die Architektur ermöglicht hier keine sicheren Transaktionen; sie macht es leicht, die Quelle von Beeinträchtigungen zu verbergen; sie erleichtert die Verbreitung illegaler Software- und Musikkopien. In diesen Kontexten zum Beispiel im Bereich eCommerce erweist sich die Unregulierbarkeit nicht als Vorteil; Unregulierbarkeit kommt dann der Entwicklungsfähigkeit des eCommerce in die Quere.

Was kann also getan werden? Es gibt viele, die meinen, dass nichts getan werden könne: dass die Unregulierbar-

keit des Internet feststeht und dass es nicht möglich ist, dies zu ändern, dass das Internet für die Dauer seines Bestehens ein unregulierbarer Raum bleiben wird, dass seine „Natur" es dazu macht.

Für die Zukunft der Freiheit im digitalen Raum ist keine Überlegung gefährlicher als dieser Glaube an eine durch Computercode garantierte Freiheit. Algorithmen sind nicht beständig. Die Architektur des digitalen Raums ist nicht vorgegeben. Unregulierbarkeit ist eine Funktion des Codes, doch dieser kann sich ändern. Andere Architekturen können über die grundlegenden TCP/IP-Protokolle gelegt werden und diese anderen Architekturen können das Netz grundlegend regulierbar machen. Im eCommerce entstehen diese anderen Architekturen; die Regierung kann helfen; beide zusammen können den Charakter des Netzes wandeln. Sie können und tun dies.

Andere Architekturen

Das, was das Netz unregulierbar macht, ist, dass schwierig festgestellt werden kann, wer jemand ist, und schwierig festzustellen ist, welche Art von Inhalt übermittelt wird. Diese beiden Eigenschaften verändern sich derzeit. Architekturen zur Erleichterung der Identifikation – oder allgemeiner zur Bestätigung von Fakten über den Nutzenden (z. B. dass jemand älter als 18, dass jemand er selbst, ein US-Amerikaner, ein Rechtsanwalt ist) – werden entwickelt und implementiert. All diese Architekturen wurden ohne Regierungserlaubnis entwickelt und zusammen können sie ein außergewöhnliches Maß an Kontrolle des Verhaltens im Netz ermöglichen. Zusammen können sie die Unregulierbarkeit des Netzes schnell beseitigen.

Können – je nachdem, wie sie geplant sind. Architekturen sind nicht binär, es gibt nicht nur eine Wahl hinsichtlich der Einrichtung einer Identifizierungsarchitektur oder einer Bewertungsarchitektur – was die Architektur ausmacht, wie ihre Kontroll- und Auswahlmechanismen beschränkt sind. Je nachdem, wie insofern entschieden wird, ist mehr oder weniger Regulierbarkeit im Spiel.

Betrachten wir zunächst Identifizierungs- oder Zertifizierungsarchitekturen. Es gibt viele Zertifizierungsarchitekturen im realen Raum. Der Führerschein ist ein einfaches Beispiel: Wenn die Polizei dich stoppt und nach deinem Führerschein fragt, fragt sie nach einer bestimmten Bestätigung, dass du zum Autofahren berechtigt bist. Diese Bestätigung gibt Auskunft über deinen Namen, dein Geschlecht, dein Alter und deinen Wohnort. All das ist nötig, weil es keine einfachere Art gibt, diese Berechtigung mit einer Person zu verbinden. Du musst all diese Fakten über dich preisgeben, um zu beweisen, dass du tatsächlich der berechtigte Inhaber des Führerscheins bist.

Bestätigungen im digitalen Raum können dagegen sehr viel eingeschränkter gestaltet sein. Wenn der Zugriff auf eine Seite nur Erwachsenen erlaubt ist, kannst du unter Nutzung von Nachweistechniken ausschließlich bestätigen, dass du ein Erwachsener bist, ohne offenzulegen, wer du bist und woher du kommst. Die Technik kann es ermöglichen, selektiv Umstände über dich zu bestätigen und zugleich andere Umstände über dich nicht zu offenbaren. Die Technik kann im digitalen Raum gemäß einer Prüfmethode der geringstmöglichen Offenbarung funktionieren, auch wenn das im realen Raum nicht möglich wäre.

Kann – je nachdem, wie sie gestaltet wurde. Es besteht jedoch keine Zwangsläufigkeit, dass die Technik sich so entwickelt. Es werden ganz andere Architekturen entwickelt – wir können sie „eine Karte zeigt alles" nennen. In derartigen Architekturen lässt sich nicht einfach begrenzen, was über ein Zertifikat offengelegt wird. Wenn du bestätigt haben möchtest, dass du ein Rechtsanwalt bist, und wenn ein Zertifikat Auskunft über Namen, Adresse, Alter, Nationalität gibt und, ob du ein Rechtsanwalt bist, so bestätigt diese Architektur nicht nur, dass du ein Anwalt bist, sondern auch all die anderen Fakten über dich, die in dem Zertifikat enthalten sind. Bei einer solchen Architektur wird „mehr" als „besser" angesehen. Nichts ermöglicht es dem Einzelnen, weniger auszuwählen.

Der Unterschied bei diesen Gestaltungsformen liegt darin, dass die eine – anders als die andere – Privatheit ermöglicht. Eine codiert Privatheit in der Identifizierungsarchitektur, indem sie dem Nutzenden eine einfache Wahl einräumt, wie viel offenbart wird; die andere vernachlässigt dieses Ziel.

Ob eine entstehende Zertifizierungsarchitektur Privatheit schützt, hängt also von der Entscheidung derjenigen ab, die kodieren. Und deren Entscheidung ist abhängig von den Anreizen, denen sie ausgesetzt sind. Gibt es keine Anreize zum Schutz von Privatheit, wenn also weder der Markt noch das Gesetz dies hinreichend fordern, dann wird dieser Code dies auch nicht vorsehen.

Das Beispiel zur Identifizierung ist nur eines unter vielen. Betrachten wir ein anderes Beispiel zum Datenschutz: RealJukeBox ist eine Technik, um Musik von einer CD auf einen Computer zu kopieren oder um Musik aus dem Netz auf die Festplatte eines Computers herunterzuladen. Im Oktober (1999, der Übersetzer) wurde bekannt, dass dieses System ein wenig neugierig ist, dass es die Festplatte des Nutzers ausspionierte und das Gefundene an das Unternehmen zurückmeldete. Natürlich tat es das heimlich. RealNetworks legte niemandem offen, dass seine Produkte persönliche Daten sammelten und übermittelten. Es passierte einfach. Als dieses Ausspionieren entdeckt wurde, verteidigte das Unternehmen zunächst die Praxis (und behauptete, dass tatsächlich keine Daten von Einzelpersonen gespeichert würden). Doch es kam schnell zu Vernunft und versprach, künftig solche Daten nicht mehr zu sammeln.

Auch dieses Problem hat seine Ursache in der Architektur. Es lässt sich im digitalen Raum nicht leicht sagen, wer was ausspioniert. Das Problem ließe sich durch eine andere Architektur lösen (so könnte z. B. eine P3P genannte Technik hier helfen), doch ist das ein Fall, wo zudem Gesetze nützlich wären. Sollte man derartige Daten als das Eigentum der Betroffenen angesehen werden, dann wäre deren Wegnahme ohne ausdrückliche Erlaubnis Diebstahl.

In diesem und in anderen Zusammenhängen verschaffen Architekturen unseren traditionellen Werten Wirkung – oder eben nicht. In jedem Fall müssen Entscheidungen getroffen werden, wie die Architektur des Internet am besten konform mit unseren Werten ausgebaut

werden soll und wie diese Architekturen mit dem Recht in Einklang zu bringen sind. Die Entscheidung über Codes und über Gesetze ist eine Entscheidung über Werte.

Werte wählen

Wollen wir also bei der Auswahl des Codes mitreden, wenn der Code unsere Werte festlegt, wollen wir uns darum kümmern, wie Werte hier in der Realität umgesetzt werden?

Zu anderen Zeiten wäre dies eine komische Frage gewesen: Selbstbestimmung ist von zentraler Bedeutung, etwa im Hinblick auf das Verfolgen der eigenen Person oder im Hinblick auf die Veränderung der unsere grundlegenden Werte beeinflussenden Bedingungen – oder, wie ich es am Anfang beschrieben habe, im Hinblick auf Regulierungen, die unsere Freiheit beeinflussen. Zu anderen Zeiten hätten wir gesagt: „Selbstverständlich wollen wir uns kümmern; selbstverständlich wollen wir mitreden."

Aber wir leben in Zeiten grundlegender Skepsis im Hinblick auf Selbstbestimmung. Unsere Zeit ist davon besessen, Dinge sich selbst zu überlassen. Es ist allgemeine Meinung, dass man das Internet sich so entwickeln lassen soll, wie die Kodierer es entwickeln: Lasst bloß die Regierung außen vor.

Diese Sichtweise ist angesichts des Charakters der Regulierung durch unsere Regierung nachvollziehbar. Angesichts der Mängel scheint es zweifellos das Beste zu sein, die Regierung herauszuhalten. Doch ist dies eine zu jeder Zeit gefährliche Nachgiebigkeit. Diese ist insbesondere jetzt gefährlich.

Wir haben nicht die Wahl, entweder zu regulieren oder nicht zu regulieren. Der Code reguliert. Er setzt Werte um, oder er lässt dies bleiben. Er ermöglicht Freiheiten oder behindert diese. Er schützt Privatheit oder fördert Überwachung. Die Menschen bestimmen, wie der Code diese Dinge tut. Code wird von Menschen geschrieben. Es geht also nicht darum, ob Menschen entscheiden, wie der digitale Raum reguliert wird. Menschen – die Kodierer – tun dies. Wir haben nur die Wahl, ob wir kollektiv etwas zu sagen haben bei deren Entscheidung – und damit bei der Festlegung, wie diese Werte reguliert werden – oder wir erlauben kollektiv den Kodierern, unsere Werte für uns auszuwählen.

Denn Folgendes ist offensichtlich: Wenn die Regierung sich zurückhält, bedeutet das nicht, dass nichts an deren Stelle tritt. Es ist nicht so, dass private Interessen interessenfrei wären, dass private Interessen kein Ziel hätten, das sie verfolgen. Wenn wir den Antiregulierungsbutton drücken, beamt uns das nicht nach Eden. Wenn die Regierungsinteressen verschwunden sind, nehmen andere Interessen deren Platz ein. Wissen wir, welches diese Interessen sind? Und sind wir so sicher, dass diese irgendwie besser wären?

Als erste Reaktion sollten wir abwarten. Es ist sinnvoll, zunächst den Markt sich entfalten zu lassen. Aber ebenso wie die Verfassung die Handlungen des Kongresses kontrolliert und begrenzt, sollten die Verfassungswerte die Aktivitäten des Marktes kontrollieren und begrenzen. Wir sollten sowohl die Gesetze des Kongresses wie auch die Produkte des Marktes auf diese Werte hin überprüfen. Wir sollten die Architektur des digitalen Raumes ebenso hinterfragen wie wir dies bei den Codizes des Kongresses tun.

Wenn wir dies nicht tun und wenn wir nicht lernen, wie wird dies tun können, wird die Relevanz unserer Verfassungstradition verblassen. Die Bedeutung unseres Bekenntnisses zu grundlegenden Werten auf der Grundlage einer selbstbewusst umgesetzten Verfassung wird verblassen. Wir werden die Gefahr ignorieren, die unsere Zeit für die Freiheiten und die überkommenen Werte mit sich bringt. Das Recht des digitalen Raums wird so sein, wie sich der digitale Raum kodiert, und wir werden auf unsere Rolle verzichtet haben, dieses Recht selbst zu setzen.

Mit freundlicher Genehmigung des Autors. Dieser weitsichtige Text aus dem Jahr 2000 findet sich im englischen Original mit dem Titel „Code is Law – On Liberty in Cyberspace" unter

http://harvardmagazine.com/2000/01/code-is-law-html.

Lawrence Lessig ist Professor für Unternehmensrecht an der Harvard Law School. Er ist Autor des Buchs „Code and Other Laws of Cyberspace" (Basic Books, http://code-is-law.org). Die Webseite des Berkman Klein Center for Internet and Society ist http://cyber.law.harvard.edu. Die persönliche Webseite von Lawrence Lessig ist http://www.lessig.org/about/.

Thilo Weichert

Die verfassungsrechtliche Dimension der Algorithmenkontrolle

Seit einigen Jahren wird über Algorithmenkontrolle diskutiert: Welche Entscheidungen dürfen unter welchen Umständen einem Computer überlassen werden und welche Relevanz darf solchen Computerentscheidungen zukommen? Wenn der Computer zum Nachteil eines Menschen entschieden hat: Welche Rechtsschutzmöglichkeiten hat der Mensch?

Diese Fragen werden auf den Feuilletonseiten seriöser Tageszeitungen umfassend erörtert; in der rechtlichen Diskussion sind sie noch nicht so richtig angekommen. Dies verblüfft, zumal Computer schon seit vielen Jahren Entscheidungen treffen und ansatzweise auch gesetzliche Regelungen anwend-

bar sind. Dass diese für unsere demokratische Informationsgesellschaft grundlegende Frage bisher allenfalls in abseitigen Fachzirkeln diskutiert wird, liegt auch am Bundesverfassungsgericht (BVerfG), das zu dieser Frage erstaunlicherweise bisher die Aussage verweigert hat und damit seine Vorreiterfunktion bei der rechtlichen Bewältigung digitaler Grundrechtsfragen nicht wahrnimmt. Mit seinen Entscheidungen zur Volkszählung 1983 und zur Online-Durchsuchung 2008 hatte das BVerfG die Grundrechte-Tür zur Informationsgesellschaft weit aufgestoßen. Es wäre dringend, dass sich das BVerfG nun auch zu den Fragen der rechtlichen Einhegung des Algorithmeneinsatzes positioniert.

Die Gesetzeslage

Eine schon fast klassisch zu bezeichnende Form einer Algorithmusentscheidung ist das Scoring zum Zweck der Bonitätsbewertung. Die Gesetzeslage hierzu war und ist weiterhin relativ klar: Gemäß § 6a BDSG-alt waren automatisierte Einzelentscheidungen auf der Grundlage von Persönlichkeitsmerkmalen nur zulässig, wenn damit dem Begehren eines Betroffenen stattgegeben wurde oder die Betroffeneninteressen durch geeignete Maßnahmen gewahrt wurden, wozu mindestens gehörte, dass dem Betroffenen der Umstand einer automatisierten Entscheidung und auf dessen Verlangen dessen wesentliche Gründe mitgeteilt und erläutert werden. Zudem hatte der Betroffene einen Anspruch auf Auskunft über „den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten. Ergänzt wurde diese Sicherung durch die Scoring-Regelung des § 28b BDSG-alt, wonach die automatisierte Entscheidung (Scoreberechnung) „unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung“ erheblich, die genutzten Daten rechtmäßig eingeführt worden und Diskriminierungen wegen der Wohnanschrift vermieden sein mussten.

Mit der neuen europäischen Datenschutz-Grundverordnung (DSGVO) änderte sich an dieser Rechtslage nichts Wesentliches: Art. 22 DSGVO erlaubt automatisierte Entscheidungen im Einzelfall einschließlich Profiling im Privatbereich nur bei „ausdrücklicher Einwilligung der betroffenen Person“ oder bei Erforderlichkeit „für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen“. Zusätzlich wird vom Verantwortlichen gefordert, dass er angemessene Maßnahmen trifft, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirken des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört“. Ergänzt wird diese Regelung in Bezug auf Bonitätsauskünfte bzw. Scoring im Wirtschaftsverkehr in § 31 BDSG-neu, der inhaltlich mit dem alten § 28b BDSG übereinstimmt. Unbestritten ist zudem nach Art. 15 DSGVO ein uneingeschränkter Auskunftsanspruch einer Person über die „sie betreffende personenbezogene Daten“, wobei in Art. 15 Abs. 1 lit. h DSGVO der Anspruch erstreckt wird bei „Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling“ auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ für die betroffene Person.

Man könnte nun meinen, dass alles gut geregelt ist: Es besteht Anspruch auf Transparenz, auf Darlegung des individuellen Standpunktes und auf Rechtsschutz für die Betroffenen. Selbst die Wissenschaftlichkeit des eingesetzten Verfahrens bleibt gesetzlich zugesichert. Die Rechtspraxis in Deutschland geht aber andere Wege. In einem grundlegenden Urteil hat das oberste deutsche Zivilgericht, der Bundesgerichtshof (BGH), am 28.01.2014 entschieden, dass bei einer Computerentscheidung zwar die einfließenden personenbezogenen Daten beauskunftet werden müssen. Das Computerergebnis müsse aber nicht begründet werden, etwa durch Mitteilungen über die für die Computerbewertung einbezogenen Vergleichsgruppen und über die Bedeutung der für das Ergebnis ausschlaggebenden Merkmale des Betroffenen.[1] Es sei nicht nötig, dass das Zustandekommen der Computerentscheidung plausibel nachvollziehbar ist.

Die Unternehmen hätten an der Geheimhaltung der „Score-Formel“, also des Algorithmus, ein schutzwürdiges Interesse. Alle damit im Zusammenhang stehenden „allgemeinen Rechengrößen“, „die herangezogenen statistischen Werte, die Gewichtung einzelner Berechnungselemente bei der Ermittlung eines Wahrscheinlichkeitswerts und die Bildung etwaiger Vergleichsgruppen“ unterlägen der Geheimhaltung, da hiervon die Wettbewerbsfähigkeit sowie der Marktwert des genutzten Produktes bzw. des einsetzenden Unternehmens abhänge. Der BGH behauptet, unter Verweis auf den EuGH[2], der Schutz der Privatsphäre solle „insbesondere durch Auskunft über die Basisdaten des Betroffenen Rechnung getragen werden“, nicht durch „konkrete Elemente“ einer Computerentscheidung. Das Auskunftsrecht dürfe nicht Geschäftsgeheimnisse berühren. Die Grenze des Zulässigen sei erst überschritten, wenn „der betroffenen Person jegliche Auskunft verweigert wird“.[3]

In der vom BGH zitierten EuGH-Entscheidung ergeben sich nicht die Schlussfolgerungen des BGH. Der EuGH hat vielmehr deutlich gemacht, dass das Recht auf Schutz der Privatsphäre voraussetzt, dass sich die betroffene Person vergewissern kann, dass ihre personenbezogenen Daten fehlerfrei verarbeitet werden und die Verarbeitung zulässig ist. Der Betroffene muss „die nötigen Nachprüfungen durchführen“ können.[4] Zwar gesteht auch der BGH zu, dem Betroffenen stehe „die schlüssige Erkenntnismöglichkeit, welche Faktoren die ausgewiesene Bewertung beeinflusst haben“, zu. Doch erstrecke sich dies nicht auf die „Nachrechenbarkeit und Überprüfbarkeit der Berechnung“.[5] Wie die schlüssige Bewertungskontrolle ohne eine Überprüfung der Berechnung möglich sein soll, bleibt das Geheimnis des BGH.

In seiner Entscheidung vom 28.01.2014 nimmt der BGH auf eine eigene Entscheidung vom 22.02.2011 Bezug[6]: „Eine darüber hinausgehende Auskunft würde zudem nicht dazu beitragen, die weitergehende Geltendmachung von Rechten nach § 35 BDSG (-alt, also von Auskunftsansprüchen, T. W.) zu ermöglichen, da sich diese nur auf personenbezogene Daten bezie-

hen. Auf eine Änderung des Scorewerts selbst besteht bei Zugrundlegung zutreffender Ausgangstatsachen ohnehin kein Anspruch."

Der BGH geht also implizit von der inzwischen völlig überholten Ansicht aus, dass es sich beim Einsatz von Algorithmen nur bei den eingegebenen Daten um personenbezogene handeln würde, nicht aber bei den Auswertungsergebnissen, die personenbezogene Konsequenzen für die Betroffenen haben. Die Debatte, inwieweit Scores, also Computerauswertungen, personenbezogen sind, wurde Anfang des Jahrtausends ausgetragen[7]; inzwischen mussten selbst die Vertreter der Auskunfteiwirtschaft nach der Verabschiedung des damals neuen § 28b im Jahr 2009 akzeptieren, dass nicht nur die sog. Basisdaten, sondern insbesondere die Computerergebnisse, z. B. die Scores, einen Personenbezug haben.[8]

Es war also, da grundlegende falsche Erwägungen zum Datenschutz angestellt worden sind, sachgerecht, dass gegen die BGH-Entscheidung im April 2014 beim BVerfG Verfassungsbeschwerde eingelegt wurde.[9] Diese hätte die Möglichkeit eröffnet, Grundlegendes zur Verfassungsgemäßheit nicht nur von Scoreberechnungen und deren -verwendung, sondern zur personenbeziehbaren Nutzung von Algorithmen generell auszuführen. Diese Hoffnung war vergeblich: Das Verfassungsbeschwerdeverfahren 1 BvR 756/14 wurde mit Nichtannahmebeschluss vom 29.05.2017 ohne weitere inhaltliche Begründung abgeschlossen. Inzwischen lagen dem BVerfG einige weitere Verfassungsbeschwerden gegen Gerichtsentscheidungen vor, in denen den Betroffenen bei der Berechnung von Scores bzw. beim Einsatz von Algorithmen ihr Grundrecht auf Datenschutz vorenthalten wurde. Soweit erkennbar, wurden all diese Beschwerden ohne weitere Begründung durch Nichtannahme abgewiesen.

Verfassungsrechtliche Bewertung

Das Grundrecht auf informationelle Selbstbestimmung[10] hat als Grundrecht auf Datenschutz in Art. 8 GRCh nicht nur europaweit eine normative Bestätigung gefunden, sondern ist zu einer prägenden verfassungsrechtlichen Säule unserer demokratischen Informationsgesellschaft geworden, die in der Rechtsprechung des BVerfG wie auch des EuGH in vieler Hinsicht weiterentwickelt wurde. Schon Art. 8 Abs. 2 S. 2 GRCh präzisiert das Grundrecht über die Betroffenenrechte wie folgt: „Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu bewirken."

Das Grundrecht auf Datenschutz gilt nicht bedingungslos, es kann eingeschränkt werden, wenn kollidierendes Verfassungsrecht dies nötig macht. Betriebs- und Geschäftsgeheimnisse werden durch das Grundrecht auf Eigentum (Art. 14 GG, Art. 17 GRCh) geschützt. In Art. 16 GRCh erfolgt eine weitere Konkretisierung durch die Anerkennung der „unternehmerischen Freiheit". Doch auch diese wirtschaftlichen Grundrechte sind nicht schrankenlos und müssen mit dem sonstigen Verfassungsrecht, zu dem das Grundrecht auf Datenschutz gehört, in praktische Konkordanz gebracht werden.

Zur unternehmerischen Freiheit und damit zum Betriebs- und Geschäftsgeheimnis kann es nicht gehören, dass falsche, diskriminierende oder sonstwie gegen das Datenschutzrecht verstoßende Daten verwendet werden. Darauf wird in § 31 Abs. 1 Nr. 1 BDSG ausdrücklich hingewiesen, wonach bei Scoringverfahren gefordert wird, dass „die Vorschriften des Datenschutzrechts eingehalten wurden". Es kann nicht im berechtigten Interesse eines Unternehmens liegen, mit falschen oder sonstwie unzulässigen Daten Entscheidungen zu treffen und damit Geschäfte zu machen.

Hinzu kommt, dass sich die individuellen Ansprüche eines Betroffenen auf die Basisdaten, die Logik des Verfahrens und die Computerergebnisse nur soweit beziehen, wie diese einen individuellen Bezug haben. Das Transparenzerfordernis erstreckt sich also nicht auf das informationstechnische Gesamtsystem, sondern beschränkt sich auf die Systemteile, mit denen eine Veränderung der Daten des Betroffenen erfolgt. Diese haben, da sie sich nur auf eine individuelle Person beziehen, keine wesentliche Marktrelevanz und können nicht als Betriebs- und Geschäftsgeheimnisse betrachtet werden. Soweit darauf übergreifende Erkenntnisse zu einem Algorithmus abgeleitet werden können, kann eine Interessenabwägung durchgeführt werden. In der Regel hat ein Betroffener kein Interesse an diesen übergreifenden Informationen, also etwa dem Quell-Code. Vielmehr ist dieser persönlichkeitsrechtlich nur daran interessiert zu erfahren, was der Algorithmus aus seinen Daten und damit mit ihm macht.

Mit dem Einsatz des Algorithmus erfolgt eine Veränderung von personenbezogenen Daten. Durch diese Veränderung können schutzwürdige Betroffeneninteressen verletzt werden. Dies geschieht nicht nur dadurch, dass falsche Basisdaten in die Auswertung eingeführt werden. Die Betroffeneninteressen können auch verletzt werden, indem der Algorithmus, also der Programmcode, auf einer korrekten Datenbasis ein persönlichkeitsverletzendes Ergebnis auswirft. So besteht ein in Scoringverfahren weit verbreiteter Programmfehler darin, dass die Wertberechnung auf einer unzureichenden Datenbasis erfolgt. Dies kann z. B. dazu führen, dass die Wohnadresse ausschlaggebend für Scoreberechnung wird, was gegen § 31 Abs. 1 Nr. 3 BDSG verstößt.[11] Fehler im Programmcode können zu falschen Daten führen, bzgl. deren beim Betroffenen ein Berichtigungsanspruch nach Art. 16 DSGVO besteht.

Für die Notwendigkeit einer Abschichtung von Geheimhaltungsinteressen eines Verantwortlichen wegen einer Auskunftspflicht im öffentlichen Interesse oder privaten Interesse eines Dritten spricht § 3 S. 5 Nr. 1-3 Verbraucherinformationsgesetz (VIG), wonach dem Verbraucher der Zugang zu bestimmten Informationen nicht mit dem Hinweis auf Betriebs- und Geschäftsgeheimnisse verweigern kann. Während hier die Gesundheit und Sicherheit des Verbrauchers das Abwägungskriterium ist, ist die Auskunft über Computerentscheidungen persönlichkeitsrechtlich begründet.

Meinungsfreiheit durch Werturteile?

Der BGH sieht dies anders, wenn er erklärt, es handele sich bei dem Rechenergebnis um ein Werturteil, bzgl. dessen kein Berichtigungsanspruch

bestünde.[12] Dabei muss er sich aber auf die Meinungsfreiheit nach Art. 5 GG und Art. 11 Abs. 1 GRCh berufen. Tatsächlich zieht der BGH diese Schlussfolgerung[13], die letztlich darauf hinausläuft, dass einem Computer bzw. dem Algorithmus ein Recht auf Meinungsfreiheit zugestanden wird.[14] Eine Computerbewertung wie das Scoring wird als eine auf Tatsachendaten beruhende subjektive Wertung angesehen.

Originäre Grundrechtsträger der Meinungsfreiheit sind natürliche Personen.[15] Dieses Grundrecht gehört zu denen, die ihrem Wesen nach aber auch auf inländische juristische Personen anwendbar sind (Art. 19 Abs. 3 GG).[16] Diesen juristischen Personen in Deutschland sind Vereinigungen aus anderen EU-Mitgliedstaaten gleichgestellt.[17] Notwendig bleibt, dass eine natürliche Person oder ein Gremium von natürliche Personen ihre Meinung für die juristische Person äußert. Nicht erfasst sind Ergebnisse von vollständig automatisiert ablaufenden Prozessen.

Zielrichtung des Grundrechtsschutzes ist die Persönlichkeitsentfaltung der sich Äußernden und seine „schlechthin konstituierende Bedeutung" für den öffentlichen Meinungsbildungsprozess und damit seine Notwendigkeit für die freiheitliche Demokratie.[18] Maschinen selbst kann keine Grundrechtsträgerschaft zugewiesen werden, selbst wenn für diese, wie bei der „künstlichen Intelligenz", das Adjektiv „intelligent" verwendet wird. Informations- und Kommunikationstechniken (IuK-Techniken) können allenfalls Meinung vermitteln, nicht aber eigenständig generieren.

Es bleibt die Frage, ob eine automatisiert generierte „Meinung" dadurch Grundrechtsschutz erlangt, dass der Betreiber des Systems anhand allgemeiner Kriterien Festlegungen vorgenommen hat, mit denen eingehende Daten verarbeitet und zu einem Ergebnis zusammengeführt werden. Eine Zurechnung kann dann angenommen werden, wenn der Verantwortliche über den Verarbeitungsprozess wie das Verarbeitungsergebnis die Kontrolle hat.[19] Für diese Kontrolle über das Verarbeitungsverfahren kann es aber nicht genügen, dass es der Wille des Verantwortlichen ist, das Computerergebnis darzustellen und den Rechenablauf zu steuern.[20]

Wie bei rechtsgeschäftlichen Erklärungen muss bei einer Meinungsäußerung ein willentlicher Akt einer Person oder von Personen stehen. Allein eine Programmierung eines Algorithmus kann nicht genügen. So fehlt es denklogisch schon dann an einer gewollten Erklärung, wenn der Dateninput vom Verantwortlichen nicht gezielt gesteuert werden kann. Erst Recht gilt dies beim Einsatz sog. künstlicher Intelligenz, bei der der eingehende Dateninput zu Programmänderungen führt, die Einfluss auf den Output, also das Ergebnis des Rechenvorgangs haben. Selbst wenn man – entgegen der hier vertretenen Meinung – kontrollierten Computerergebnissen eines Systembetreibers eine diesem zuzurechnende Meinung attestieren würde, kann und darf diese für die demokratische Meinungsbildung nicht als relevant anerkannt werden.

Der Schutz der Meinungsfreiheit zielt auf den Inhalt der Meinung ab. Dieser kann sich auch auf den wirtschaftlichen Wettbewerb und eine kommerzielle Meinungsäußerung beziehen. Nicht geschützt sind insofern aber reine kommerzielle Verwertungsaktionen von Daten oder geäußerten Meinungen. Insofern können lediglich die wirtschaftlichen und Unternehmensrechte nach Art. 12, 14 GG bzw. Art. 15-17 GRCh geltend gemacht werden.[21]

Datenrichtigkeit

Im Datenschutzrecht gilt der auch aus Art. 8 Abs. 2 S. 2 GRCh abzuleitende Grundsatz der Datenrichtigkeit. Der hierzu bestehende Anspruch auf Datenkorrektur ergibt sich aus Art. 16 DSGVO. Gemäß Art. 5 Abs. 1 lit. d DSGVO haben personenbezogene Daten generell „sachlich richtig und erforderlichenfalls auf dem neuesten Stand" zu sein.[22] Es sind „angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden". Die Regelung deutet darauf hin, dass es keine objektive Richtigkeit gibt, sondern dass diese im Zusammenhang mit dem jeweils verfolgten Zweck gesehen werden muss.

Beim Zusammenführen von Daten für Computerentscheidungen müssen die jeweiligen Kontexte und Erhebungszwecke berücksichtigt werden, um keine falschen Ergebnisse zu erlangen. Diese Umstände sind oft selbst nicht digital erfasst und müssen daher für valide Analysen digital ergänzt werden. Wegen der hohen Komplexität der Sachverhalte und der gegenseitigen Abhängigkeiten können ohne eine solche Kontextualisierung Algorithmen zu objektiv falschen Ergebnissen führen.[23]

Für die Richtigkeit der per Algorithmus errechneten Ergebnisse spielt neben der Datenqualität, also der Richtigkeit der eingeführten Einzeldaten, auch deren Repräsentativität eine zentrale Rolle. Werden Ergebnisse einzelnen Personen zugeordnet, so hat die Repräsentativität nicht nur eine wissenschaftliche, sondern in Bezug auf die Richtigkeit auch eine datenschutzrechtliche Relevanz. Für die Repräsentativität eines Ergebnisses kommt es wesentlich auf die Vergleichsgruppe an, deren Daten zur Grundlage für die Bewertung herangezogen werden. Werden z. B. für eine Bonitätsbewertung als Vergleichsgruppe Personen mit ausschließlich geringen Risiken herangezogen, so berechnet ein Algorithmus zu einer Person mit einem gering höheren, aber immer noch sehr geringen Risiko zwangsläufig eine schlechte Bonität. Der Ausschluss der Auskunftspflicht auf die Vergleichsgruppe durch den BGH ignorierte deren Relevanz für die Richtigkeit des Algorithmenergebnisses und damit für den Datenschutz der Betroffenen.

Für die Richtigkeit einer Computerberechnung ist es weiterhin relevant, welche Relevanz der Algorithmus einem Merkmal beimisst. Dies wurde im Hinblick auf die Wohnadresse ausdrücklich vom Gesetzgeber klargestellt, als er bestimmte, dass die Wohnadresse nicht allein für eine Bonitätsbewertung ausschlaggebend sein darf (§ 31 Abs. 1 Nr. 4 BDSG). Wird ein irrelevantes Merkmal von einem Algorithmus als ausschlaggebend eingestuft, so ist dies nicht eine subjektive Bewertung des Computers bzw. des Programmierers, sondern schlicht objektiv falsch.

Demokratie- und Rechtsstaatsprinzip

Angesichts des Umstands, dass Computerentscheidungen in immer stärke-

rem Maße auf demokratische Meinungsbildungsprozesse Einfluss nehmen, etwa durch von Bots produzierte Meldungen, welche die freie menschliche Meinungsbildung beeinträchtigen, kann und darf auch durch natürliche und vor allem juristische Personen initiierten Computerentscheidungen kein Meinungsschutz zugesprochen werden.[24]

Gemäß Art. 20 Abs. 1 GG ist die Bundesrepublik Deutschland ein demokratischer und sozialer Bundesstaat. Gemäß Art. 2 EUV sind die Werte, auf denen sich die Union gründet, „die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte. Als Konkretisierung der genannten Prinzipien werden in Art. 2 EUV „Pluralismus, Toleranz, Gerechtigkeit, Solidarität und Nichtdiskriminierung" genannt. Haben komplexe Algorithmen Auswirkungen auf diese demokratischen Werte, so kann dies staatliche Interventionen rechtfertigen.

Betroffene haben einen Justizgewährleistungsanspruch nach Art. 19 Abs. 4, 20 Abs. 3 GG bzw. Art. 47 GRCh. Erfolgt durch die Computerentscheidung eine Persönlichkeitsverletzung, so muss der Betroffene die Möglichkeit haben, diese vor Gericht geltend zu machen. Voraussetzung dieser Geltendmachung ist, dass er und letztlich das Gericht das berechnete Ergebnis überprüfen, d. h. dass die Unrichtigkeit eines Computerergebnisses nachweisen kann.

Lawrence Lessig hat schon in seinem Aufsatz „Code ist Law" aus dem Jahr 2000 darauf hingewiesen, dass mit zunehmender Digitalisierung rechnergestützte Vorgaben immer mehr die Regeln unseres gesellschaftlichen Zusammenlebens bestimmen und damit die Wahrnehmung unserer Freiheitsrechte einschränken, ohne dass hierüber bewusste politische, geschweige denn transparente und mehrheitlich getroffene Entscheidungen zugrunde liegen.[25] Das Ergebnis sind „unkontrollierbare" und „unverantwortliche" Entscheidungen mit evtl. hoher gesellschaftlicher oder andere Menschen betreffender Relevanz.

Insbesondere beim Einsatz von Big Data und sog. Künstlicher Intelligenz entsteht ein Transparenz-, Kontroll- und Entscheidungsproblem: Basiert eine automatisiert vorbereitete oder getroffene Entscheidung nicht auf einer nachvollziehbaren „Wenn-dann-Datenauswertung", sondern auf einem digital generierten komplexen Algorithmus, so kann dies dazu führen, dass die Gründe für diese Entscheidung nicht mehr nachvollzogen und kontrolliert werden können. Selbstlernende Algorithmen lassen sich nicht mehr hinreichend protokollieren bzw. dokumentieren. Selbst im Fall einer nachvollziehbaren Protokollierung kann oft keine einem Menschen oder einer Institution zuordenbare (rechtliche) Verantwortlichkeit begründet werden. Die Verantwortlichkeit für die Programmierung sog. künstlicher Intelligenz begründet im bestehenden Rechtsregime nicht zwangsläufig die (rechtliche) Verantwortlichkeit für eine auf dieser Grundlage getroffene (rechtlich relevante) Entscheidung. Selbst für den Fall einer theoretisch begründbaren Haftung des Programmierers bleibt das praktische Problem bestehen, dass wegen der Arbeitsteilung bei einer komplexen Programmcode-Generierung eine Verantwortungszuordnung in der Praxis oft nicht möglich ist.

Diese Defizite wirken sich direkt auf die gerichtliche Kontrolle durch die Justiz (Art. 19 Abs. 4 GG, Art. 47 GRCh) sowie die demokratische Kontrolle durch Parlamente aus (Art. 20 Abs. 1, 2 GG). Richter wie Parlamentarier werden mit technisch geschaffenen Fakten konfrontiert, deren Wirkzusammenhänge von ihnen nicht nachvollzogen, geschweige denn verstanden werden können. Die generierten Fakten sind mit dem Nimbus der digitalen Objektivität und Wissenschaftlichkeit behaftet. Diese normative Kraft des Faktischen entsteht aber nicht naturwüchsig oder zufällig. Sie wird bestimmt durch diejenigen, in deren Interesse die Algorithmen entwickelt und eingesetzt werden, die dann mehr oder weniger freiwillig und unreflektiert von Verwaltung, Wirtschaft und Menschen genutzt werden. Ergebnis ist die Beeinträchtigung der verfassungsrechtlich gewährleisteten Prinzipien von Rechtsstaatlichkeit und Demokratie.

Diskriminierungsverbote

Das deutsche wie auch das europäische Verfassungsrecht enthält spezifische Diskriminierungsverbote: Art. 3 Abs. 3 GG verbietet die Benachteiligung oder Bevorzugung „wegen seines Geschlechts, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen". Art. 21 GRCh konkretisiert und erweitert dies durch zusätzliche Benennung folgender, die Diskriminierung verbietender Merkmale: Hautfarbe, ethnische oder soziale Herkunft, genetische Merkmale, Weltanschauung, Zugehörigkeit zu einer nationalen Minderheit, Vermögen, Geburt, Behinderung, Alter und sexuelle Ausrichtung.[26]

Diese Diskriminierungsverbote haben im Hinblick auf Algorithmenentscheidungen eine zweifache Relevanz: einerseits verbieten sie grundsätzlich die Nutzung der genannten Merkmale als einfließende Bewertungsmerkmale, soweit damit eine nicht gerechtfertigte Wirkung (Bevorzugung wie Benachteiligung) gegenüber den Betroffenen verbunden ist. D. h. rein erkenntnissuchende Analysen werden durch die Diskriminierungsverbote nicht untersagt. Zu beachten ist aber, dass die Grenzen zwischen Erkenntnis und daraus resultierender Diskriminierung abstrakt nicht eindeutig bestimmbar sind. Eine Einzelfallbewertung ist nötig. Diskriminierung erfolgt durch Algorithmen dadurch schnell, dass diese nicht zwischen Korrelation und Kausalität unterscheiden können.[27] Schwer bestimmbar sind die Grenzen zwischen legitimer Differenzierung und unzulässiger Diskriminierung. Besteht eine Diskriminierungsabsicht, so ist diese in jedem Fall verboten. Besteht aber ein begründeter Sachzusammenhang, so kann sich hieraus eine Rechtfertigung ergeben. Dies gilt insbesondere, wenn die Differenzierung eine rechtliche Grundlage hat.[28]

Eine verfassungsrechtlich verbotene Diskriminierung kann sich auch daraus ergeben, dass nicht die in die Datenauswertung einfließenden, wohl aber die Ergebnisse eine nicht gerechtfertigte Differenzierung zur Folge haben. Ein äußerlich objektiver Algorithmus kann zu einer objektiven Benachteiligung wegen eines der genannten Diskriminierungsmerkmale führen.[29] Derartige Wirkungen werden beispielsweise bei Internetauswertungen[30] oder bei gene-

tischen Untersuchungen immer wieder dokumentiert.[31]

Algorithmenkontrolle

Aus den obigen Ausführungen ergibt sich, dass Algorithmenkontrolle nicht nur zulässig, sondern verfassungsrechtlich geboten sein kann. Dies gilt insbesondere bei Konstellationen, wo ein starkes Ungleichgewicht zwischen dem den Algorithmus einsetzenden Unternehmen und den Betroffenen besteht. Die staatliche Schutzpflicht gebietet, die Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes für die Betroffenen sowie grundrechtssichernde Prozesse bereitzustellen. Dies gilt insbesondere dann, wenn private Stellen ein solches ökonomisches, technisches oder organisatorisches Gewicht haben, dass sie die informationellen Vorgänge zu Personen (Betroffenen) faktisch einseitig bestimmen können.[32]

Für Algorithmenkontrollen gibt es bisher keine direkten Erfahrungen. Prozedural bestehen unterschiedliche Möglichkeiten zur Gewährleistung der Verfassungskonformität von im Alltag eingesetzten Algorithmen.[33] Im Folgenden soll ein Vorschlag präzisiert werden, der an einem normativ vorgegeben Verfahren ansetzt, für das es bisher aber noch keine bzw. nur wenig praktische Umsetzungen gibt: die Zertifizierung nach Art. 42 DSGVO. Dieses Verfahren muss sich nicht auf den Nachweis einer Datenschutzkonformität im engeren Sinne beschränken, sondern kann gemäß Art. 1 Abs. 2 DSGVO umfassend den Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen" einschließlich deren gesellschaftlicher Funktion umfassen.[34]

Deutschland steht es offen, auf der Grundlage von Art. 42 DSGVO ein Zertifizierungsverfahren zu etablieren, bei dem die Einhaltung der verfassungsrechtlichen Anforderungen an den Einsatz von Algorithmen geprüft und bestätigt wird. In einem ersten Schritt sollten Kriterien erarbeitet werden, nach denen derartige Zertifizierungen durchgeführt werden. Dies kann durch die Datenschutzaufsichtsbehörden erfolgen (Art. 42 Abs. 5 DSGVO). Dabei sollten schon in einem frühen Stadium Differenzierungen nach den jeweiligen Einsatzbereichen vorgesehen werden. Der Einsatz von Algorithmen im Gesundheitsbereich ist nach anderen Maßstäben zu bewerten als z. B. in der Werbebranche.

In einem ersten Schritt mag es zur Sammeln von Erfahrungen sinnvoll sein, die Zertifizierungen auf einer freiwilligen Basis anzubieten (Art. 42 Abs. 3 DSGVO). Es ist aber nicht ausgeschlossen, dass für spezifische Zwecke und Gefahrenlagen auf zusätzlicher gesetzlicher Basis obligatorische Zertifizierungen vorgesehen werden.[35]

Es ist an der Zeit, dass der Schritt von der Diskussion über die Notwendigkeit von Algorithmenkontrolle zur tatsächlichen Erprobung von Verfahren und dann zur normativen Festlegung gegangen wird. Dies ist primär die Aufgabe der Politik, insbesondere dann, wenn sich wie hier die Rechtsprechung scheut, Festlegungen aus der Verfassung abzuleiten. Angeknüpft werden kann und sollte hier bei der Datenschutzaufsicht, wo juristische und technische Kompetenz sowie die Aufgabe des digitalen Grundrechtsschutzes zusammengeführt werden.[36] Umfassender als bei der allgemeinen Datenschutzkontrolle sind bei der Algorithmenkontrolle ein Monitoring und ein dauerndes Risikomanagement möglich und auch nötig.[37] Dabei ist nicht nur automatisierte, sondern immer auch menschliche Supervision gefordert.[38] Die dafür zuständigen Aufsichtsbehörden müssen hierzu aber mit den nötigen Ressourcen ausgestattet werden. Wünschenswert wären europäische Projekte, Erfahrungen und Vorgaben. Solange diese ausstehen, muss und kann ein Staat wie Deutschland, der sich der Digitalisierung der Gesellschaft verschrieben hat, voraus gehen.

1 BGH 28.01.2014 – VI ZR 156/13, NJW 2014, 1235 = NVwZ 2014, 747 = K&R 2014, 269 = ZIP 2014, 476 = MDR 2014, 412 = VersR 2014, 461 = WM 2014, 452 = MMR 2014, 489 = MIR 2014, Dok. 025 = BB 2014, 842 = DB 2014, 588 = DuD 2014, 341 = DANA 1/2014, 47; kritisch dazu Spindler DB 2018, 46; Schulte am Hülse/Timm NJW 2014, 1238 f.; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/GP Forschungsgruppe (ULD/GPF), Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen, 2014, S. 44 ff..

2 EuGH 07.05.2009 – C-533/07, Rn. 49 f., EuZW 2009, 548.

3 BGH 28.01.2014 – VI ZR 156/13 (Fn. 1) Rn. 33.

4 EuGH Rn. 49; dazu auch ULD, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, S. 46, https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3.

5 BGH 28.01.2014 – VI ZR 156/13 (Fn. 1), Rn. 25 f.

6 BGH 22.02.2011 – VI ZR 120/10, Rn. 8 ff., NJW 2011, 2204 = DuD 2011, 498 = RDV 2011, 188 = DSB 6/2011, 16 = VersR 2011, 632 = MDR 2011, 598 = NZM 2011, 726 = WM 2011, 1187 = MMR 2011, 409 = BB 2011, 1169 = DB 2011, 873 = afp 2011, 259 = afp 2012, 217.

7 ULD (Kamp/Weichert), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, 2005, S. 66 f. m. w. N., https://www.datenschutzzentrum.de/uploads/projekte/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf.

8 Relativierend immer noch Kamlah in Plath, BDSG DSGVO, 2. Aufl. 2016, § 28b Rn. 6.

9 Schufa-Klägerin zieht vor das Verfassungsgericht, www.handelsblatt.com 11.04.2014.

10 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419.

11 Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, § 31 BDSG Rn. 20.

12 Dazu Däubler in Däubler u. a. (Fn. 11) Art. 16 DSGVO Rn. 7.

13 BGH U. v. 28.01.2014 – VI ZR 156/13 (Fn. 1) Rn. 30 mit Verweis auf BGH 22.02.2011 – VI ZR 120/10 (Fn. 6) Rn. 8 ff.

14 ULD/GPF, Scoring nach der Datenschutznovelle (Fn. 1) S. 50 f. m. w. N.

15 Starck in von Mangoldt/Klein, Kommentar zum Grundgesetz, 6. Aufl. 2010, Bd. 1, Art. 5 Abs. 1, 2 Rn. 178.

16 Starck in von Mangoldt/Klein (Fn. 15), Art. 5 Abs. 1, 2 Rn. 181.

17 BVerfGE 129, 78 = NJW 2011, 3428 Rn. 57

18 BVerfGE 5, 205; 7, 219; 12, 125; 20, 174 ff.; 25, 265; Starck in von Mangoldt/Klein (Fn. 15) Art. 5 Abs. 1, 2, Rn. 11; Bethge in Sachs, GG, 6. Aufl. 2011, Art. 5 Rn. 22 m. w. N.

19 Milstein/Lippold, NVwZ 2013, 185 mit Verweis auf BGH 29.04.2010 – I ZR 69/08, Rn. 20, BGHZ 185, 291 = NJW

2010, 2731 = ZIP 2010, 5 = MDR 2010, 884 = GRUR 2010, 628 = MMR 2010, 475 = MIR 2010, Dok. 078 = BB 2010, 1161 = K&R 2010, 501 = ZUM 2010, 580 = afp 2010, 265.

20 Milstein/Lippold NVwZ 2013, 185.

21 BVerfG 19.11.1985 – 1 BvR 934/82, Rn. 68, BVerfGE 71, 175; BVerfG 22.01.1997 – 2 BvR 1915/91 Rn. 47, BVerfGE 95, 181 f.

22 Zur Sanktionierbarkeit Hoeren ZD 2016, 462.

23 Siehe hierzu den Beitrag von Spiekermann, S. 128.

24 Siehe die Beispiele bei Hoffmann-Riem AöR 142 (2017), 11 ff.

25 Lessig, Code is Law – On Liberty in Cyberspace, http://harvardmagazine.com/2000/01/code-is-law-html; hier übersetzt abgedruckt ab S. 130; ähnlich Boehme/Neßler NJW 2017, 3033.

26 Wischmeyer AöR 143 (2018, 26 ff.; zur Anwendbarkeit des Allgemeinen Gleichbehandlungsgesetzes (AGG) Weichert, Big Data im Gesundheitsbereich, 2018, Kap. 6.14, http://www.abida.de/de/blog-item/gutachten-big-data-im-gesundheitsbereich; Spindler DB 2018, 46; Martini JZ 2017, 1021.

27 Weichert, Big Data im Gesundheitsbereich (Fn. 26) Kap. 5; Wischmeyer AöR 143, 35 sowie in Fn. 48;

28 BVerfG 22.05.1975 – BvL 13/73, Rn. 93-96, BVerfGE 39, 368.

29 Martini JZ 2017, 1018

30 Weichert, Big Data im Gesundheitsbereich (Fn. 26) Kap. 5.4. zu Autocomplete BGH 14.05.2013 – VI ZR 269/12, NJW 2013, 2348 ff. = JZ 2013, 789 ff. = DuD 2013, 663 ff. = MMR 2013, 535 ff. = DANA 2013, 132 f.; LG Wien 24.11.2016 – 13 Cg 16/16t-31, ZD 2016,7, 379; Rassismusvorwurf gegen Google wegen „Autocomplete"-Suchangebot, DANA 2012, 89 f.

31 Zur genetischen Forensik vgl. Weichert, Vorgänge Nr. 218 (2/2017), S. 129 ff.

32 BVerfG 23.10.2006 – 1 BvR 2027/02, Schweigepflichtentbindung, NJW 2007, 576; Papier NJW 2017, 3030; Wischmeyer AöR 143 (2018), 20; Schliesky/Hoffmann u. a., Schutzpflichten und Drittwirkung, 2014.

33 Siehe hierzu die Vorschläge von Ehrig/Blinn in diesem Heft, S. 138; Martini JZ 2017, 1025.

34 Weichert in Däubler u. a. (Fn. 11) Art. 1 DSGVO Rn. 15.

35 Weichert in Däubler u. a. (Fn. 11) Art. 42 Rn. 29; Spindler DB 2018, 46.

36 Zur Aufsichtsthematik Spindler DB 2018, 46

37 Martini JZ 2017, 1021 f.

38 Wischmeyer AöR 143 (2018), 14 f.

Lina Ehrig, Miika Blinn

Algorithmenbasierte Entscheidungsprozesse und Verbraucherschutz

Algorithmen haben schon heute großen Einfluss auf unser Leben und unseren Alltag. Sie sind keine Zukunftsmusik, sie sind Realität – nicht nur bei Google, Facebook und Co. Verbraucher kommen zum Beispiel damit in Berührung, wenn sie einen Kredit beantragen. Der Algorithmus berechnet dann die Wahrscheinlichkeit des finanziellen Ausfalls – und entscheidet damit, ob der Verbraucher[1] einen Kredit bekommt und zu welchen Konditionen. Auch in der Finanzanlageberatung können Algorithmen zum Einsatz kommen. Manche Fintechs bieten Kunden in Deutschland an, ihr Vermögen algorithmenbasiert zu verwalten. Auch einige Krankenzusatzversicherungen, Online-Händler sowie Softwarehersteller beim autonomen Fahren setzen auf algorithmenbasierte Entscheidungsprozesse.

Im Zentrum der aktuellen Debatte stehen algorithmenbasierte Entscheidungsprozesse (Algorithmic Decision Making, im Folgenden ADM-Prozesse)[2], die auf der Grundlage von Big Data erfolgen können. Sie sind von besonderem Interesse, da die Zahl der betroffenen Verbraucher potenziell sehr hoch sein kann; oft bei mangelnder Transparenz über die jeweiligen ADM-Prozesse. Es ist davon auszugehen, dass diese Prozesse zunehmend entscheidenden Einfluss auf Fragen der Lebensgestaltung, auf Teilhabemöglichkeiten, Konsumentscheidungen und Autonomie jedes Einzelnen sowie auf die Gesellschaft insgesamt haben werden.

Der Verbraucherschutz muss diese Entwicklung positiv begleiten, aber auch auf Risiken hinweisen. Die Chancen von ADM-Prozessen liegen beispielsweise darin, dass die Teilhabe erhöht werden kann, wenn Verbraucher einen breiten Zugang zu personalisierten Angeboten und Diensten erhalten, die bisher aus Kostengründen nur wenigen zur Verfügung standen[3]. Auch die Konsistenz von Entscheidungen kann verbessert werden, da bei ADM-Prozessen immer nach den gleichen Vorgaben aufgrund festgelegter Kriterien entschieden wird. Menschliche Fehler durch verzerrte Wahrnehmung und persönliche Präferenzen können so gegebenenfalls reduziert werden[4]. Die Risiken können unter anderem Sicherheitsrisiken, Gefährdung der Privatsphäre, Steigerung der Informationsasymmetrie zwischen Verbrauchern und Unternehmen, eingeschränkte materielle und soziale Teilhabe von Individuen und Gruppen (z. B. Diskriminierung), Manipulation beziehungsweise unbewusste Beeinflussung individueller Entscheidungen sowie die Aushebelung des Wettbewerbs umfassen.

Wo sich Risiken abzeichnen, muss die Politik diese durch kluge Maßnahmen minimieren. Ziel muss es sein, dass auch in einer Welt selbstlernender Algorithmen rechtliche Rahmenbedingungen eingehalten werden und die Entscheidungssouveränität sowie die informationelle Selbstbestimmung von Verbrauchern gewährleistet sind. Das

ist nur möglich, wenn ADM-Prozesse durch Menschen kontrollierbar sind und bleiben.

Diese Ziele können jedoch kaum erreicht werden, solange ADM-Prozesse ein hohes Maß an Intransparenz aufweisen.

Wichtig ist, dass alle verstehen: Algorithmen fallen nicht vom Himmel. Menschen mit individuellen Wertevorstellungen und unterschiedlichen Interessen programmieren sie. Das alles passiert jeden Tag, ohne dass wir über Transparenz, Diskriminierungsschutz, Überprüfbarkeit, Kontrolle und Korrigierbarkeit der Verfahren sprechen. Viele Unternehmen verweigern es, einen Einblick darüber zu geben, auf welche Weise Entscheidungen zustande kommen – oftmals mit Verweis auf ihre Geschäftsgeheimnisse. Diese Intransparenz führt zu einer problematischen Wissensasymmetrie zwischen Verbrauchern und Unternehmen. Dadurch steigt das Risiko, dass Verbraucher diskriminiert und manipuliert werden.

Deshalb brauchen wir ein geeignetes, staatlich legitimiertes Kontrollsystem, welches sich durch Vielschichtigkeit auszeichnet und nicht aus einer einzigen Institution besteht. Es könnte mehrere Elemente umfassen, deren Zusammenwirkung eine angemessene Kontrolle sicherstellen kann. Elemente eines solchen Kontrollsystems könnten beispielsweise ein betrieblicher Algorithmenbeauftragter (in Anlehnung an die Datenschutzbeauftragten), der die Einhaltung von Qualitätsstandards gewährleistet, ein erweitertes Informationsfreiheitsgesetz, staatliche Stellen wie etwa die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin[5]) oder Vereine, die aufgrund einer staatlichen Beauftragung arbeiten (TÜV), sein. Hierdurch soll es möglich sein, relevante ADM-Prozesse hinsichtlich Rechtskonformität (beispielsweise Diskriminierungsverbot, Lauterkeitsrecht und Datenschutzrecht), Sachgerechtheit der Anwendung sowie individueller und gesellschaftlicher Auswirkungen einzusehen und zu überprüfen.

Das verbreitete Misstrauen von Verbrauchern gegenüber ADM-Prozessen und der gleichzeitige Wunsch nach größerer Transparenz dieser Systeme und deren unabhängige Kontrolle[6] legt den Schluss nahe, dass die Etablierung eines effektiven Kontrollsystems eine maßgebliche Voraussetzung für die Schaffung von Vertrauen und breite Akzeptanz von ADM-Prozessen ist - und somit für die Realisierung der Chancen, die diese bieten.

Darüber hinaus brauchen wir dringend eine Debatte, wie wir mit den gesellschaftlichen und ethischen Folgen von ADM-Prozessen umgehen wollen, etwa dem Risiko eines fortschreitenden Verlusts menschlicher Autonomie. Ergebnis einer solchen Debatte könnten beispielsweise Prinzipien eines Ethik-by-Design sein, nach denen Ersteller von ADM-Prozessen rechtliche und ethische Grundsätze schon bei der Programmierung und beim ADM-Design berücksichtigen müssen. Die Bundesregierung muss diese Debatte antreiben und im Rahmen der Datenethikkommission Lösungsvorschläge anbieten.

1 Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

2 Ein algorithmenbasierter Entscheidungsprozess umfasst weitaus mehr als den reinen Programmcode oder Algorithmus: „Algorithmische Entscheidungsfindung bezeichnet den Gesamtprozess von der Datenerfassung über die Datenanalyse bis hin zur Deutung und Interpretation der Ergebnisse und der Ableitung einer Entscheidung oder einer Entscheidungsempfehlung aus den Ergebnissen“. Vgl. Vieth, Kilian; Wagner, Ben: Teilhabe, ausgerechnet, 2017, Arbeitspapier im Auftrag der Bertelsmann Stiftung, S. 10, https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/teilhabe-ausgerechnet, 21.09.2017

3 Wenn beispielsweise Algorithmen zum Portfoliomanagement von Geldanlagen eingesetzt werden, können diese bereits Vermögen ab 5000 Euro profitabel managen, was bei menschlichen Portfoliomanagern für die Finanzdienstleister nicht rentabel wäre. Vgl. Frankfurter Allgemeine Zeitung: Wenn der Algorithmus das Vermögen verwaltet, 17.08.2016, http://www.faz.net/aktuell/finanzen/fonds-mehr/automatisierte-finanzberatung-wenn-der-algorithmus-das-vermoegen-verwaltet-14384953.html, 03.10.2017

4 Zu Heuristiken und verzerrten Entscheidungen in Gerichtsverfahren vgl. Peer, Eyal; Gamliel, Eyal: Heuristics and Bias in Judicial Decisions, Court Review, Vol. 49, 114-118, http://aja.ncsc.dni.us/publications/courtrv/cr49-2/CR49-2Peer.pdf, aufgerufen am 05.12.2017. Neben Effizienzgewinnen wird von Unternehmensseite der Einsatz von automatisierten Entscheidungen in Bewerbungsverfahren auch damit begründet, dass sie helfen sollen Verzerrungen im Bewerbungsprozess zu reduzieren. Vgl. Lechtleitner, Sven: Wenn der Algorithmus entscheidet, 04.09.2017, https://www.humanresourcesmanager.de/news/wenn-der-algorithmus-entscheidet.html, 05.12.2017

5 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Algorithmischer Handel und Hochfrequenzhandel, 2016, https://www.bafin.de/DE/Aufsicht/BoersenMaerkte/Hochfrequenzhandel/high_frequency_trading_node.html, 15.08.2017

6 Fischer, Sarah und Petersen,Thomas: Was Deutschland über Algorithmen weiß und denkt, Ergebnisse einer repräsentativen Bevölkerungsumfrage, 2018, Arbeitspapier im Auftrag der Bertelsmann Stiftung, S. 24 ff., https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/was-deutschland-ueber-algorithmen-weiss-und-denkt/, 12.07.2018

Klaus-Jürgen Roth

Datenschutzaufsicht und Politik

- zur Regulierung des Auswahlprozesses der Leitung von Aufsichtsbehörden am Beispiel Schleswig-Holsteins -

Die Wahl und die Benennung von Datenschutzbeauftragten als „Mitglieder“ von Datenschutzaufsichtsbehörden erfolgt über bisher wenig hinterfragte politische Prozesse. Da damit auch eine inhaltliche Festlegung beim Datenschutz verbunden ist, sollte hier mehr Transparenz und demokratischer Diskurs erfolgen. Am Beispiel der Wahl des langjährigen DVD-Vorsitzenden und heutigen DVD-Vorstandsmitglieds Thilo Weichert zum Vorstand des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) wird diese Forderung untermauert.

1 Einleitung: EuGH-Urteil und unabhängige Aufsicht

Kurz vor dem Wirksamwerden der europäischen Datenschutz-Grundverordnung (DSGVO) Ende Mai 2018 verabschiedete der schleswig-holsteinische Landtag ein neues Landesdatenschutzgesetz (LDSG SH) sowie ein Gesetz zur Errichtung eines Unabhängigen Landeszentrums für Datenschutz (ULD-G).[1] Kurz nach Wirksamwerden der DSGVO verkündete der Europäische Gerichtshof (EuGH) sein Urteil zur Verantwortlichkeit bei Internet-Dienstleistungen, konkret der Fanpagebetreiber für die durch Facebook durchgeführte Datenverarbeitung.[2]

Beide Ereignisse haben nicht nur zeitlich und über die DSGVO eine Verbindung, sondern auch durch die Klagegegner im EuGH-Verfahren. Diesem Verfahren liegt eine Verfügung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) gegenüber der Wirtschaftsakademie Schleswig-Holstein GmbH (WAK) zugrunde. Die WAK ist eine privatwirtschaftliche Tochter der Industrie- und Handelskammer Schleswig-Holstein (IHK), also der öffentlich-rechtlichen Organisiertheit der Wirtschaft des Landes. Das ULD hatte, in einer Art Musterverfahren, der WAK, stellvertretend für die Wirtschaft des Landes, den Facebook-Fanpagebetrieb untersagt, weil die dadurch ausgelöste Datenverarbeitung bei Facebook gegen Datenschutz verstieß. Das EuGH-Urteil, das sich voll der Position des ULD anschloss, erging auf eine Vorlage des Bundesverwaltungsgerichts.[3] Zuvor war das ULD gegenüber der WAK vor dem Verwaltungsgericht[4] und dem Oberverwaltungsgericht Schleswig-Holstein[5] unterlegen.

Das EuGH-Verfahren ist nicht nur inhaltlich bemerkenswert, sondern auch durch den Umstand, dass sich hier eine Datenschutzaufsichtsbehörde erklärtermaßen nicht nur der Position der organisierten Wirtschaft, sondern auch der Regierung des eigenen Bundeslandes widersetzte, die ebenso wie die WAK mehrere Facebook-Fanpages betreibt. Diese stellte dadurch ihre Unabhängigkeit unter Beweis.

So schließt sich der Kreis zum neuen ULD-G, mit dem Qualität und Unabhängigkeit der Datenschutzaufsicht in Schleswig-Holstein gewährleistet werden sollen, so wie dies in Art. 8 Abs. 3 GRCh und in den Art. 52 u. 53 DSGVO gefordert wird. Das Facebook-Verfahren war der zentrale Ansatzpunkt der Kritik am damaligen Leiter des ULD Thilo Weichert. Diese war wiederum der zentrale Gegenstand der politischen Debatte um die Besetzung der Position der ULD-Leitung.

In § 2 Abs. 1 ULD-G heißt es nun: „Der Landtag wählt auf Vorschlag der Fraktionen ohne Aussprache die Landesbeauftragte oder den Landesbeauftragten mit mehr als der Hälfte seiner Mitglieder für die Dauer von 6 Jahren. Eine einmalige Widerwahl in zulässig.“ Hinter dieser eher formal daher kommenden Regelung versteckt sich ein heftiger, viele Jahre dauernder politischer Streit über die Benennung der ULD-Leitung.

2 Ausgangslage

Eine dem ULD-G ganz ähnliche Regelung galt mit § 35 Abs. 1 LDSG SH seit dem Jahr 2000. Diese unterschied sich inhaltlich nur dadurch, dass anstelle der sechs- eine fünfjährige Amtszeit vorgesehen war. Am 29.04.2004 wurde Thilo Weichert auf Vorschlag der regierenden Fraktionen SPD und Grüne in offener Abstimmung mit den Stimmen von SPD, Grünen, SSW (Südschleswigscher Wählerverband) und FDP gegen die Stimmen der CDU als Nachfolger des bisherigen ULD-Leiters Helmut Bäumler zum Landesbeauftragten gewählt.[6] Weichert war von 1984 bis 1986 Landtagsabgeordneter der Grünen im Landtag Baden-Württemberg. Er übernahm, nachdem er zuvor 5 Jahre lang Stellvertreter von Bäumler war, fristgemäß am 01.09.2004 dessen Funktion. Schon in seiner ersten Amtsperiode erwies sich Weichert als engagierter Datenschützer, weshalb es Konflikte mit den jeweiligen Landesregierungen gab, etwa mit dem SPD-Innenminister Ralf Stegner bei der Novellierung des Polizeirechts 2006.[7]

3 Erste Wiederwahl

Als im Jahr 2008 erneut die Wahl der ULD-Leitung anstand, hatte sich die Regierungsmehrheit geändert und wurde nun von der CDU und der SPD gestellt. Kurz nach Ablauf der offiziellen Amtsperiode wurde Weichert in einer offenen Abstimmung auf Antrag der Oppositionsfraktionen FDP, Grüne, SSW einstimmig im Amt bestätigt.[8]

Dieses Ergebnis war nicht selbstverständlich. Zeitlich im Zusammenhang mit der Vorstellung des ULD-Tätigkeitsberichtes war es zu einer Vielzahl von Pu-

blikationen über die weitere Besetzung der ULD-Leitung gekommen. CDU- und SPD-Fraktion hatten zuvor untereinander vereinbart, das Vorschlagsrecht hierfür solle bei der CDU liegen, nachdem die SPD die Stelle der Bürgerbeauftragten des Landes besetzt hatte. Als CDU-Alternative wurde der stellvertretende Vorsitzende der CDU-Fraktion Thomas Strietzel genannt, der aber keinerlei Erfahrungen beim Datenschutz nachweisen konnte. Daraufhin schlugen FDP, Grüne und SSW als ihren Kandidaten Weichert vor. Gemäß dem stellvertretenden SSW-Vorsitzende Lars Harms habe es Schleswig-Holstein Weichert zu verdanken, dass das Land auf dem ersten Platz in der „Datenschutz-Bundesliga" stehe. Die SPD, mit der die CDU noch vor der Wiederwahl Weicherts die Koalition auflöste, schwieg sich zunächst aus und unterstützte Weichert aber nach dem Koalitionsbruch offensiv. Dies veranlasste die CDU zu beschließen, Weichert mitzuwählen und quasi im Gegenzug „in Weicherts Amt Stellen zu kürzen". Die Zustimmung der CDU zur Wiederwahl Weicherts wurde zugleich „als Signal an die Ökopartei" für eine mögliche schwarz-grüne Koalition nach der anstehenden Landtagswahl interpretiert.[9]

4 Gesetzesänderungen

War also die Motivation des Wahlverhaltens 2009 bei der Benennung der ULD-Leitung bei vielen Fraktionen wenig fachlich und überwiegend parteipolitisch bestimmt, so war dieses Phänomen bei den Wahlen 2014/2015 zur ULD-Leitung noch bestimmender. Im § 35 Abs. 1 S. 2 LDSG-SH war vorgesehen, dass eine Wiederwahl nur einmal zulässig ist. Weichert war interessiert, nach Ablauf seiner zweiten Amtszeit mit einem Alter von 60 Jahren eine weitere Amtsperiode anzuhängen, weshalb er gegenüber den Landtagsfraktionen anregte, den Wiederwahlausschluss im LDSG zu streichen. Bei den Oppositionsparteien stieß er hierzu auf positive Resonanz.

4.1 Unabhängige Aufsicht

2010/2011 kam die Unabhängigkeit der Datenschutzaufsicht dadurch unfreiwillig auf die Tagesordnung des Landtags Schleswig-Holstein, weil der EuGH mit Urteil vom 09.03.2010 die Bundesrepublik Deutschland wegen eines Verstoßes gegen die europäische Datenschutzrichtlinie (EG-DSRl) verurteilte. Deutschland hatte mit seinen Organisationsstrukturen für die Datenschutzaufsicht nicht die in Art. 28 Abs. 1 UAbs. 2 EG-DSRl geforderte Unabhängigkeit umgesetzt.[10] Dies galt nicht nur für das Amt des Bundesbeauftragten, sondern ebenso für die Aufsichtsbehörden der Länder und damit auch für Schleswig-Holstein. Zwecks Umsetzung dieser europarechtlichen Vorgabe brachten die Regierungsfraktionen CDU und FDP 2011 einen Entwurf zur Änderung des LDSG ein.[11] Weitergehende Novellierungsvorschläge des ULD wurden von den Regierungsfraktionen nicht aufgegriffen.

4.2 LDSG-Novelle

Die weitergehenden ULD-Vorschläge wurden zumindest teilweise parallel durch einen Regierungsentwurf zur Änderung des LDSG aufgegriffen.[12] Bei der Behandlung des Vorschlags im Innen- und Rechtsausschuss beantragte die Fraktion des SSW in einem Änderungsantrag, § 35 Abs. 1 S. 2 dahingehend zu ändern, dass die Wiederwahl des ULD-Leiters nicht beschränkt wird.[13] Der damalige datenschutzpolitische Sprecher der CDU-Fraktion Michael von Abercron sowie die Sprecherin der FDP-Fraktion Ingrid Brand-Hückstädt hatten zuvor persönlich signalisiert, dass sie der Streichung der Wiederwahlausschlusses zustimmen würden. Erstaunlicherweise stimmten dann aber in der Sitzung des Innen- und Rechtsausschuss am 30.11.2011 sämtliche CDU- und FDP-Abgeordneten gegen die Antrag des SSW; SPD, Grüne, SSW und Linke stimmten dafür.[14] Damit blieb es vorläufig bei der auf einmal beschränkten Wiederwahlmöglichkeit. Die erste Auseinandersetzung um die Wiederwahlmöglichkeit der ULD-Leitung in Schleswig-Holstein fällt zeitlich zusammen mit dem Versuch des ULD, die datenschutzwidrigen Aktivitäten von Facebook rechtlich in den Griff zu bekommen. Das ULD und dessen Leiter sahen sich deshalb massiven Angriffen insbesondere aus der Wirtschaft des Landes ausgesetzt.[15]

Nach der Wahl am 06.05.2012 für den 18. schleswig-holsteinischen Landtag hatten sich die Mehrheiten gedreht. Die Linken schieden wieder aus; die Piraten zogen mit 6 Abgeordneten ins Parlament ein und der neue Ministerpräsident Torsten Albig hatte mit den Fraktionen von SPD, Grünen und SSW eine hauchdünne Mehrheit von einer Stimme im Landtag. Diese wurde aber vorläufig nicht genutzt, um verbleibenden Novellierungsbedarf im LDSG nachzuholen. Erst kurz vor Ablauf der Amtszeit von Weichert stellten die Fraktionen fest, dass eine Wahl des Datenschutzbeauftragten ansteht. Als erste brachte die Piraten-Fraktion Januar 2014 einen Gesetzentwurf ein, wonach die Wahl in zeitlicher Nähe zum Ablauf der vorangegangenen Amtszeit erfolgen soll; die Wahl solle „auf Vorschlag eines Ausschusses, dessen Zusammensetzung und Verfahren der Landtag in seiner Geschäftsordnung regelt", erfolgen oder auf Vorschlag der Fraktionen. Es solle eine öffentliche Ausschreibung und eine Anhörung der Bewerberinnen und Bewerber in öffentlicher Sitzung geben.[16] Daraufhin wurden sich die Regierungsfraktionen SPD, Grüne und SSW einig, dass eine Wiederwahl von Weichert wünschenswert, aber gesetzlich bisher ausgeschlossen ist und beantragten im Februar 2014, in § 35 Abs. 1 S. 2 LDSG die Worte „nur einmal" zu streichen.[17] In Reaktion hierauf wiederum beantragte die CDU-Fraktion, für die Wahl des ULD-Leiters als Datenschutzbeauftragten eine 2/3-Mehrheit statt der bisherigen absoluten Mehrheit erforderlich zu machen.[18] Vorbild waren entsprechende Regelungen in Niedersachsen und Sachsen-Anhalt. In der Sitzung des Innen- und Rechtsausschusses vom 29.10.2014 wurde der CDU-Entwurf mit den Stimmen der Regierungsfraktionen gegen die Stimmen von CDU und Piraten bei Enthaltung der FDP abgelehnt.[19]

Der Entwurf der Regierungsfraktionen wurde von der Opposition mit dem Titel „Lex Weichert" versehen und öffentlich massiv angegriffen. Der CDU-Abgeordnete Axel Bernstein brachte die Kritik in einem Satz auf den Punkt: „Zur Versorgung eines grünen Parteifreundes wird der Datenschutz dauerhaft auf Facebook reduziert". Um neue Entwicklungen zu beobachten und voranzutreiben, bedür-

fe es ab und zu eines Personalwechsels.[20] Vor der politischen Auseinandersetzung stand eine mehr oder weniger wissenschaftliche Diskussion um die Entwürfe der Piraten und der Regierungsfraktionen. Hieran beteiligt wurden das ULD[21], der Landesbeauftagte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV)[22], der Landesbeauftragte für den Datenschutz Niedersachsen[23], Prof. Joachim Krause von der Universität Kiel (CAU)[24], Prof. Hans Peter Bull[25], die Deutsche Vereinigung für Datenschutz e. V. (DVD)[26], der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI)[27], die Arbeitsgemeinschaft der kommunalen Landesverbände[28], Transparency International (TI)[29] und Prof. Florian Becker (CAU)[30]. Der LfDI MV, das ULD und die DVD betonten in ihren Stellungnahmen, dass es für die Qualität der Tätigkeit des ULD-Leiters darauf ankäme, dass dieser fachlich kompetent ist, wofür ein transparenter Auswahlprozess förderlich ist; ein Auswechseln nach einer gewissen Amtszeit sei dagegen untergeordnet. Am 18.06.2014 beschloss der Landtag in zweiter Lesung den Regierungsentwurf mit der uneingeschränkten Wiederwahlmöglichkeit und lehnte den Piratenentwurf ab.[31] Das Gesetz trat einen Tag nach seiner Verkündung am 27.06.2014 in Kraft.[32]

5 Gescheiterte Wahl

Am 10.07.2014 stand die Wahl des Landesbeauftragten für den Datenschutz auf der Tagesordnung des Landtags. Neben dem Kandidaten der Regierungsfraktionen Weichert[33] hatte die FDP kurzfristig ihren früheren Landtagsabgeordneten Rechtsanwalt Gerrit Koch zur Wahl gestellt.[34] Bei der geheimen Wahl wurden 69 Stimmen abgegeben; davon entfielen 34 auf Weichert, 30 auf Koch bei 5 Enthaltungen.[35] Damit wären die Wetten, die die Abgeordneten Wolfgang Kubicki und Uli König auf der Sitzung am 19.02.2014 abgeboten haben, nämlich dass nach einer Änderung des LDSG Weichert gewählt würde[36], verloren worden.

Die Nichtwahl Weicherts blieb in der 18. Legislaturperiode der einzige Fall, bei dem die Einstimmenmehrheit der rot-grün-blauen Koalition sich nicht gegen die Opposition durchgesetzt hat. Sie erinnerte an die Nichtwahl von Heide Simonis zur Ministerpräsidentin Schleswig-Holsteins am 17.03.2005, bei der auch eine Stimme ausschlaggebend war. In Analogie zur Bezeichnung „Heide-Mord“ hierfür[37] war nun vom „Thilo-Mord“ die Rede.[38]

Nach der Nichtwahl Weicherts wurde in den Medien spekuliert, weshalb diese erfolgte, so etwa Erich Maletzke: „Der Abweichler zielte zwar auf Weichert, wollte aber in Wirklichkeit Torsten Albig treffen. Ein Regierungschef hat in den eigenen Reihen immer Gegner. Aus den unterschiedlichsten Gründen. Manchmal sind sie sogar sehr privatpersönlicher Art. Nicht auszuschließen ist auch, dass jemand dem in der SPD-Fraktion nur mäßig beliebten Vorsitzenden Stegner einen kleinen Denkzettel geben wollte.“[39] Als Grund für das Ergebnis nannten viele auch das „Durchpeitschen“ der Wiederwahlmöglichkeit.[40] Selbst die Verletzung von Etikette wurde als möglicher Grund genannt, weil dem FDP-Kandidaten Koch von Seiten des Regierungslagers die Möglichkeit der Vorstellung verweigert wurde.[41] Interessant für die Bewertung des Vorgangs ist auch ein Kommentar von Ministerpräsident Albig (SPD), der es als „extrem ärgerlich und unprofessionell“ bezeichnete, „dass jemand durch sein Verhalten in dieser politisch ja nicht besonders relevanten Personalfrage schlechte Signale aussendet“.[42]

5.1 Mehrheitssuche

In einem Interview legte SPD-Fraktionschef Ralf Stegner seine Strategie offen, wie „es bei der Wahl des Datenschutzbeauftragten eine Mehrheit über SPD, Grüne und SSW hinaus geben kann“: „Außerdem werde ich mich mit den Kollegen der Oppositionsparteien treffen. Es stehen ja weitere Personalentscheidungen an, etwa die Leitung einer neu formierten Landeszentrale für politische Bildung.“[43] Die FDP spekulierte aber mehr mit einer Besetzung eines Postens im Senat des Landesrechnungshofes. Der FDP-Kandidat Christian Albrecht scheiterte bei seiner Wahl am 13.11.2014 an den Gegenstimmen der Koalitionsfraktionen.[44] Albrecht wurde später 2016 bei unveränderten Mehrheiten im Landtag dann doch noch in diese Position einstimmig gewählt.[45]

Entgegen ersten Spekulationen kam es zunächst nach der Sommerpause 2014 zu keinen weiteren öffentlichen Aktivitäten hinsichtlich der ULD-Leitung; Weichert übte die Funktion kommissarisch weiter aus. Im September 2014 hatte das OVG Schleswig-Holstein gegen das ULD im Streit um Facebook-Fanpages entschieden.[46] Bewegung kam in den Auswahlvorgang für die ULD-Leitung erst wieder mit der Präsentation des ULD-Tätigkeitsberichts am 23.03.2015, wodurch das Thema Datenschutz wieder in den Fokus der Aufmerksamkeit der Landespolitik geriet. Es wurde nun von allen Landtagsfraktionen gemeinsam ein „offizielles Interessensbekundungsverfahren“ gestartet, das bis zum 30.04.2015 geschlossen werden sollte. CDU und FDP signalisierten aber schon öffentlich, Weichert nicht wählen zu wollen, da das Land „einen neuen Landesdatenschutzbeauftragten“ brauche und „Betriebsblindheit“ zu verhindern sei.[47] Unklar war zunächst die Position der Piraten, die inhaltlich ihre politische Argumentation oft und gerne mit den Positionen Weichert begründeten. Für deren Fraktionsvorsitzenden Patrick Breyer war jedoch die Haltung von Weichert nicht kompromisslos genug, etwa weil dieser eine differenzierte Bewertung bei der Vorratsdatenspeicherung von Telekommunikationsdaten oder bei polizeilichen Befugnissen eingefordert hatte.

Auf das Interessenbekundgungsverfahren meldeten sich viele Interessierte. CDU und FDP meinten ein Coup landen zu können, indem sie sich zum Abschluss des Bewerbungsverfahrens für die Wahl der grünen Plöner Kreistagspolitikerin Kirsten Bock aussprachen. Die Juristin Bock war zum damaligen Zeitpunkt 11 Jahre lang beim ULD tätig. FDP-Fraktionschef Wolfgang Kubicki meinte „dass es möglich sein wird, für Frau Bock eine Mehrheit zu bekommen.“ Sie selbst erklärte das Standard-Datenschutzmodell aus dem ULD zu ihrem „Herzblutprojekt“ Sie wurde als Expertin für europäisches und internationales Datenschutzrecht präsentiert.[48] In einem Internet-Kommentar war aber zu lesen, Bock sei „ULD-intern ein rotes Tuch“, weshalb dem ULD im Fall ihrer Wahl „eine Zerreißprobe“ drohe.[49]

5.2 Wahl von Marit Hansen

In dieser Situation entschied sich die seit 2008 als Stellvertreterin in der ULD-Leitung tätige Informatikerin Marit Hansen, sich für das Amt bereit zu stellen. Hansen arbeitete damals schon seit 20 Jahren für das ULD und hatte sich durch Forschungsprojekte im Bereich des Datenschutzes international Renommee verschafft. Weichert erklärte, zu ihren Gunsten auf eine weitere Kandidatur zu verzichten.

Nach einer Vorstellung von Hansen bei den Fraktionen der Regierungsparteien wie der Piraten erklärten diese, dass sie Hansen als Kandidatin vorschlagen werden. Hierauf wiederum erklärte Hans-Jörg Arp für die CDU-Fraktion „Die Lex Weichert ist ab heute überflüssig. Thilo Weichert hat in den vergangenen Jahren durch – seiner Kampagne gegen Facebook dienende – Klagen vielen kleinen und mittelständischen Unternehmen in Schleswig-Holstein das Leben schwer gemacht. Nun endlich ist eine von SPD, Grünen und SSW zu verantwortende jahrelange Hängepartie beendet“.[50]

Weichert selbst kommentierte die Vorgänge wie folgt: „Der Datenschutz ist Spielball der Politik“. Zur Relevanz des Facebook-Verfahrens für seinen nicht freiwilligen Rückzug meine er: „Facebook war sicher eine sehr nachhaltige Auseinandersetzung, aber nicht mein größter Kampf“. Er wies darauf hin, dass die rechtliche Auseinandersetzung am 12.12.2015 beim BVerwG in die nächste Runde gehen werde. Zu seiner bisherigen Stellvertreterin und späteren Nachfolgerin meine er: „Ich wüsste niemand besseres.“ Mit ihr seien Kontinuität und Qualität gesichert.[51]

Danach konnte es nicht schnell genug gehen: Auf der letzten Sitzung vor der Sommerpause am 15.07.2015 wurde die Wahl der Landesdatenschutzbeauftragten auf die Tagesordnung gesetzt. Die CDU und die FDP verzichteten auf einen eigenen Wahlvorschlag. Der Wahlvorschlag Marit Hansen von SPD/Grüne, Privaten und SSW[52] erhielt in geheimer Abstimmung von den 68 abgegebenen und gültigen Stimmen 49 Ja- und 11 Nein-Stimmen bei 8 Enthaltungen.[53] Hansen hatte also nicht nur die Stimmen der antragstellenden Fraktionen, sondern auch welche von der CDU und der FDP erhalten. Zwar hieß es in § 35 Abs. 1 S. 1 LDSG, dass die Wahl der Landesbeauftragten „ohne Aussprache“ stattfindet. Der nächste Tagesordnungspunkt nach der Wahl Hansens war aber zum 35. Tätigkeitsbericht 2015 des ULD, den die Redner aller Fraktionen dazu nutzten, die vergangene Arbeit von Weichert zu würdigen. Dabei wurde der Stil von Weichert bewertet als offen und fair (Bernstein CDU), als unbequem, kompetent, streitlustig und öffentlichkeitswirksam. Im Zentrum der Bewertungen der Abgeordneten von Weicherts Engagement als ULD-Leiter stand sein Engagement zu Facebook, das teils positiv, teils kritisch gewürdigt wurde.[54] Bei der offiziellen Verabschiedung von Weichert am 03.09.2015 wurde von Ministerpräsident Torsten Albig nochmals betont, wie wichtig es gewesen sei, dass das ULD und Weichert die Diskussion um die Datenmacht Facebook angestoßen habe.[55]

6 Nochmals: Gesetzesänderung

Marit Hansen leitet seitdem unangefochten das ULD. Doch spielten die Themen der Auseinandersetzung um die ULD-Leitung weiterhin eine Rolle. So veröffentlichte der Fraktionsvorsitzende der Piraten vor der Landtagswahl am 2017 Breyer „Mein persönliches Highlight der vergangenen fünf Jahre“: „Die Küstenkoalition scheiterte mit dem Versuch, den ehemaligen Landesdatenschutzbeauftragten wiederzuwählen. Stattdessen haben wir PIRATEN eine öffentliche Ausschreibung des Amts durchgesetzt“.[56] Bei der Landtagswahl am 07.05.2017 erzielten die Piraten 1,2% der Wählerstimmen und zogen nicht wieder ins Parlament ein.

Auch hinsichtlich der Transparenz der Wahl der ULD-Leitung erwies sich das Highlight Breyers nicht als nachhaltig: Das zur Umsetzung der DSGVO von einer schwarz-grün-gelben Koalition verabschiedete ULD-G sieht nun in § 5 Abs. 1 weder Transparenz noch öffentliche Ausschreibung vor. In Satz 2 heißt es: „Eine einmalige Wiederwahl ist zulässig.“ Die einzige Konzession von CDU und FDP an die Grünen scheint zu sein, dass anstelle der zunächst geplanten 5jährigen eine 6jährige Amtszeit der ULD-Leitung vorgesehen ist.[57]

7 Schlussfolgerungen

Die Diskussion über die Datenschutzaufsicht ist mit der DSGVO in eine neue Phase eingetreten. Art. 53 Abs. 1 DS-GVO verpflichtet die Mitgliedstaaten, das Mitglied ihrer Aufsichtsbehörden „im Wege eines transparenten Verfahrens“ zu ernennen. Dessen ungeachtet enthält nicht nur das LDSG SH bzw. das ULD-G, sondern enthalten alle allgemeinen deutschen Datenschutzgesetze zur Umsetzung der DSGVO keine Regelung zur Transparenz der Leitungen der Aufsichtsbehörden. Damit verstoßen die Gesetzgeber ganz offensichtlich gegen die expliziten DSGVO-Vorgaben.[58]

Dessen ungeachtet erfolgte die Diskussion um die Besetzung der ULD-Leitung – unfreiwillig – von der ersten Wiederwahl Weicherts an in einer breiten Öffentlichkeit. Dies war dem Umstand zuzuschreiben, dass die Besetzungen jedes Mal Gegenstand parteipolitischer Auseinandersetzungen waren. Natürlich dient die parlamentarische Auswahl der Leitungen der Aufsichtsbehörden nicht nur der Feststellung von „Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten“, sondern auch einer datenschutzpolitischen Priorisierung.[59] Letztlich dient die Wahl der Leitung deren demokratischer Legitimation. Es gibt keine politisch neutrale Verteidigung digitaler Grundrechte.

Das hier ausführlich dargestellte Fallbeispiel zu Schleswig-Holstein ist Beleg dafür, dass bei der Wahl des „Mitglieds“ oft keine fachlichen Aspekte ausschlaggebend sind. Einige der politischen Äußerungen deuten sogar darauf hin, dass subjektive persönliche Aspekte für das politische Handeln im Vordergrund standen. Soweit bei der Nichtwahl Weicherts fachliche Aspekte eine Rolle spielten, wurden diese von dessen Umgang mit Facebook bestimmt, der insbesondere von der rechtlich geforderten Unabhängigkeit von Politik und Wirtschaft zeugte. Es ist Ironie der Geschichte, dass gerade dieser politisch massiv angegriffene Umgang letztlich vom EuGH in seinem Urteil vom 05.06.2018 bestätigt wurde.[60] Der Vorgang zu Facebook und dessen spätere Bewertung durch den EuGH unterstreicht die Notwendigkeit der Unabhängigkeit der Da-

tenschutzaufsicht – auch und insbesondere von der Politik, nicht nur von den zu kontrollierenden Stellen.

Bei einer Analyse des konkreten Verhaltens der verschiedenen politischen Fraktionen im oben analysierten Fall erweist sich zunächst, dass die CDU eine eher datenschutzkritische und wirtschaftsfreundliche Position vertrat und vertritt. Dies ist wenig überraschend. Eine aufsichtsfreundliche Position vertreten und vertraten die Grünen sowie der SSW. Die SPD wiederum demonstrierte ein teilweise engagiertes, zugleich aber auch ein stark taktisches Verhältnis zum Datenschutz. Verblüffend war das Verhalten von FDP und Piraten, zwei programmatisch dem Datenschutz eher zugeneigten Parteien. Für sie war offenbar das Vorführen der jeweiligen Landesregierung, der sie nicht angehörten, zentral für ihr Verhalten. Das „Lex Weichert“ wurde weiterhin bekämpft, auch nachdem es in Kraft getreten war und kurzfristig keine politische Relevanz mehr hatte. Inhaltliche Erwägungen zum Datenschutz wurden zurückgestellt zugunsten formaler und letztlich parteipolitischer Erwägungen. Die Frage der Wiederwahlmöglichkeit spielte bisher für die politischen Parteien im Bund oder in Bundesländern – außer im konkreten Fall – keine Rolle.

Letztlich ist die Transparenz des Benennungsverfahrens die einzige begrenzte Garantie für eine Sicherung weitest gehender Unabhängigkeit. Die in den Ländern Sachsen-Anhalt und Niedersachsen geltende Regelung, für die Wahl des „Mitglieds“ eine Zweidrittelmehrheit zu fordern, führt genau in die entgegen gesetzte Richtung: Die Nichtwahl Nils Leopolds durch den Landtag Sachsen-Anhalt im März und im Mai 2018 ist hierfür ein Beleg. Die Wahl der Datenschutzaufsicht scheint geradezu dafür prädestiniert zu sein, für parteipolitische datenschutzfremde Zwecke missbraucht zu werden. Qualifizierte Mehrheiten sind im Sinne des angestrebten Grundrechtsschutzes nicht gemeinwohlfördernd.[61]

Die Schlussfolgerung, die aus dem oben dargestellten Fallbeispiel gezogen werden kann, ist zu versuchen, den parteipolitischen Einfluss auf die Besetzung der Aufsichtsbehörden zurückzudrängen. Zwar sollte ausgeschlossen sein, dass, wie noch kurz vor dem Wirksamwerden der DSGVO praktiziert, die Besetzung dieser Ämter ausschließlich nach politischen Kriterien erfolgen und nicht nach Qualifikation. Als Alternative dazu kommt nur eine verstärkte öffentliche Debatte in Betracht. Öffentliche Ausschreibungen, wie sie z. B. für den Europäischen Datenschutzbeauftragten von Anfang an üblich sind, sollten der Mindeststandard sein.[62] Ergänzt werden sollte dies in jedem Fall durch eine öffentliche Anhörung der Kandidatinnen und Kandidaten, bevor eine demokratisch legitimierte Wahl stattfindet.

Nach der Wahl ist vor der Wahl: Eine kritische Begleitung der Tätigkeit der Aufsichtsbehörden durch Medien und Nichtregierungsorganisationen ist dringender denn je, nachdem die Datenschutzaufsicht in der DSGVO mit mehr Befugnissen ausgestattet wurde. Durch die öffentliche Begleitung der Aufsichtstätigkeit wird letztlich die wichtigste Entscheidungsgrundlage für die Frage geschaffen, ob eine das Amt inhabende Person erneut gewählt werden soll oder nicht. Dies gilt nicht nur für die kritische Berichterstattung durch die Medien, sondern auch für die wissenschaftliche Durchdringung des Verhältnisses zwischen Politik, Wirtschaft und Datenschutzaufsicht.

1 Errichtungsgesetz ULG, G. v. 02.05.2018, GVBl. Sch.H. Nr. 8/2018 v. 17.05.2018, S. 162 ff.

2 EuGH U. v. 05.06.2018 – C-210/16.

3 BVerwG B. v. 25.02.2016 – 1 C 28.14, CR 2016, 729 = K&R 2016, 437 = DuD 2016, 537.

4 VG Schleswig U. v. 09.10.2013 – 8 A 14/12, K&R 2013, 824 = ZD 2014, 51.

5 OVG SH 04.09.2014 – 4 LB 20/13, ZD 2014, 643 = K&R 2014, 831.

6 Landtag (LT) Schleswig-Holstein (SH), Pl.Pr. 15/113 S./8772, Antrag LT-Drs. 15/3364.

7 ULD, 28. Tätigkeitsbericht (TB) 2006, Kap. 4.2.1 (S. 31 ff.); 29. TB 2007, Kap. 4.2.1 (S. 32 ff.).

8 LT SH, Pl.Pr. 16/123, S. 9101; Antrag LT-Drs. 16/2688.

9 Höver, CDU sendet Koalitionssignale, www.shz.de 11.07.2009; Hammer, CDU macht Weg für Weicherts Widerwahl frei, Lübecker Nachrichten 09.09.2009, 7; Borchers, Einigung um Datenschutzposten in Schleswig-Holstein in Sicht, www.heise.de 13.07.2009; Borchers, Debatte um Datenschutzposten in Schleswig-Holstein, www.heise.de 01.04.2009; CDU will Weichert loswerden, SPD schweigt dazu, Eckernförder Ztg. 01.04.2009, 3.

10 EuGH U. v. 09.03.2010 – C-518/07, NJW 2010, 1205.

11 LT-Drs. 17/1599 v. 15.06.2011.

12 LT-Drs. 17/1698 v. 10.08.2011; zu den ULD-Vorschlägen 34. TB 2013, Kap. 1.1 (S. 9 f .).

13 LT-Umdruck 17/2658 v. 31.08.2011.

14 Schleswig-Holsteinischer Landtag Innen- und Rechtsausschuss, Niederschrift 17. WP – 79 Sitzung 30.11.2011, S. 19 ff.

15 34. TB ULD 2013 Kap. 2.2, 7.1 (S. 16 ff., 111 ff.); Weichert, Datenschutz als Geschäftsmodell – der Fall Facebook, DuD 2012, 719 ff.; Wirtschaft zwischen Nord- und Ostsee (IHK-Zeitschrift), Rimpf, Nachteile für regionale Unternehmen Heft 10/2011, 32, Legband, „Wer nicht kämpft, hat schon verloren“, zitiert IHK-Präsident Vater Heft 02/2012, 25, Fanseiten bleiben zulässig, Heft 11/2013, 51.

16 LT-Drs. 18/1472 v. 15.01.2014.

17 LT-Drs. 18/1558 (neu) v. 11.02.2014; Plenardebatte dazu Pl.Pr. 18/48 v. 19.02.2014 S. 3941 ff.

18 LT-Drs. 18/1764 v. 28.03.2014, Art. 2.

19 LT-Drs. 18/2397 v. 05.11.2014.

20 PM CDU-Fraktion Nr. 069/14 v. 10.02.2014; zitiert von Abg. Eichstädt Pl.Pr. 18/48 S. 3943; Bernstein S. 3944.

21 Stellungnahme (Stn.) v. 10.03.2014, LT-Umdruck 18'/2534.

22 Stn. v. 10.03.2014, LT-Umdruck 18/2522

23 Stn. v. 11.03.2014, LT-Umdruck 18/2535.

24 Stn. v. 28.03.2014, LT-Umdruck 18/2646.

25 Stn. v. 31.03.2014, LT-Umdruck.

26 Stn. v. 09.04.2014, LT-Umdruck 18/2711.

27 Stn. V. 09.04.2014, LT-Umdruck 18/2782.

28 Stn. V. 28.03.2014, LT-Umdruck 18/2647.

29 Stn. v. 28.04.2014, LT-Umdruck 18/2764.

30 Stn. v. 07.05.2015, LT-Umdruck 18/2783.

31 Pl.Pr. 18/60 v. 18.06.2014 S. 4856.

32 G. v. 19.06.2014, GVBl. SH 2014, 105.

33 LT-Drs. 18/2102 v. 26.06.2014.

34 LT-Drs. 18/2125 v. 08.07.2014.

35 Pl.Pr. 18/64 . 10.07.2014 S. 5296.

36 Pl.Pr. 18/48 S. 3948, 3951.

37 Kammholz/Ehrenstein, Interview mit Heide Simonis u. Peter Harry Carstensen, www.welt.de 08.03.2015; Werner, „Heide-Mord" – Die Macht politische Gerüchte, www.welt.de 24.06.2016.

38 Maletzke, Die Rückkehr des „Heide-Mörders" www.shz.de 13.07.2014.

39 Die Rückkehr des „Heide-Mörders" www.shz.de 13.07.2014.

40 Hammer, Eine Koalition leckt ihre Wunden, Lübecker Nachrichten 12.07.2014.

41 Widmann, Thilo Weichert Datenschützer in Kiel und Opfer der politischen Zustände dort, SZ 12./13.07.2014, 4.

42 Baethge, „Extrem ärgerlich und unprofessionell" Schleswig-Holsteinische Landeszeitung (SHZ) 12.07.2014

43 Christen/Thiede, Interview mit Stegner, „Ich bevorzuge Klartext", KN 04.08.2014, 9.

44 LT-Drs. 18/2280, Pl.Pr. 18/74 v. 13.11.2014 S. 6136.

45 FDP-Mann Albrecht nun doch im Rechnungshof, http://www.landtag.ltsh.de, 09.10.2016.

46 OVG SH 04.09.2014 – 4 LB 20/13, ZD 2014, 643 = K&R 2014, 831.

47 So CDU-Fraktionsvorsitzender Daniel Günther und parlamentarischer FDP-Geschäftsführer Heiner Garg, in Tiede, Weichert kritisiert Stillstand, www.kn-online.de 24.03.2015.

48 CDU und FDP wollen grüne Datenschützerin, Kieler Nachrichten 19.06.2015, 10; Schulzki-Haddouti, CDU/FDP für Grüne als Datenschutzbeauftragte, www.heise.de 18.06.2015; CDU/FDP für Grüne als Datenschutzbeauftragte, www.kn-online.de 18.6.2018.

49 Blatand, Selten dämlicher Vorschlag von CDU und FDP, www.heise.de 18.06.2018.

50 PM CDU-Fraktion v. 30.06.2015, Hans-Jörg Arp zum ULD: Die Lex Weichert ist ab heute überflüssig.

51 Klohn, Deutschlands prominentester Datenschutz geht: „Der Datenschutz ist Spielball der Politik" www.heise.de 11.07.2015.

52 LT-Drs. 18/3184 v. 02.07.2015.

53 Pl.Pr. 18/93 v. 15.07.2015 S. 7914.

54 Pl.Pr. 18/93 v. 15.07.2015 S. 7914-7920.

55 https://www.datenschutzzentrum.de/artikel/948-Verabschiedung-von-Dr.-Thilo-Weichert-und-Amtsantritt-von-Marit-Hansen.html#extended.

56 Der Landtag Nr. 1/2017, April 2017, Bilanz Patrick Breyer (Piraten) S. 10, vgl. www.schattenblick.de.

57 G. v. 02.05.2018, GVBl. SH v. 17.05.2018 S. 162; Synopse mit ursprünglichem Entwurf LT-Drs. 19/664 v. 26.04.2018.

58 Netzwerk Datenschutzexpertise, Zum Auswahlprozess von Datenschutzbeauftragten als Leitung der Aufsichtsbehörden, www.netzwerk-datenschutzexpertise.de 17.11.2016, S. 16.

59 Nguyen in Gola, DS-GVO, 2017, Art. 53 Rn. 4.; Ziebarth in Sydow, Europäische Datenschutzgrundverordnung, 2017, Art. 53 Rn. 18; Thomé VuR 2015, 133; Piltz K&R 2016, 781.

60 EuGH U. v. 05.06.2018 – C-210/16; s. o. 1.

61 DANA 2/2018, 101, 1108 f.; Pressemitteilung der DVD v. 29.05.2018, DVD: Sachsen-Anhalt Datenschutz-Entwicklungsland!?

62 Selmayr in Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 53 Rn. 5.



Bild: iStock

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Handy-Auswertung bei Flüchtlingen bringt wenig

Seit September 2017 wertet das Bundesamt für Migration und Flüchtlinge (BAMF) die Daten auf den Smartphones von Flüchtlingen aus, um festzustellen, ob diese bei ihren Angaben zu Herkunft, Fluchtweg und Kontakten die Unwahrheit sagen (DANA 2/2017, 101 f.). Juni 2018 wurden erstmals Erkenntnisse vorgelegt, was die aufwändige Aktion bringt: offensichtlich nicht viel. Die Auswertung der Auswertung belegte nicht den verbreiteten Verdacht, dass Flüchtlinge in größerem Ausmaß versuchen zu tricksen oder zu lügen bei ihren Angaben zu Identität, Herkunft und Staatsangehörigkeit. In einer Antwort der Bundesregierung auf die Anfrage der Linksfraktion wird das Ergebnis der Pilotphase von September 2017 bis Mai 2018 erstmals zusammengefasst. Nur in etwa 100 Fällen haben sich danach in den neun Monaten Hinweise auf Widersprüche ergeben zwischen den Handydaten und den eigenen Angaben der Asylsuchenden. In diesem Zeitraum wurden rund 230.000 Asylanträge entschieden.

Das Auslesen von Mobiltelefonen war im vergangenen Jahr trotz heftiger Proteste von DatenschützerInnen und FlüchtlingshelferInnen eingeführt worden, um etwa mittels Telefonverbindungen und Fotos verlässlichere Informationen zur Herkunft von Asylsuchenden zu bekommen (DANA 2/2017, 101 f.). Wer als Flüchtling keinen Pass vorlegt, wird um die Herausgabe seines Mobiltelefons gebeten. Die Geräte werden ausgelesen, die erlangten Informationen in einem „Datentresor" gespeichert und nur dann verwendet, wenn Identität und Herkunft des Antragstellers unklar sind. Offenbar helfen diese Informationen aus den Mobiltelefonen nur in den seltensten Fällen den Entscheidern des BAMF weiter.

Von September 2017 bis Mai 2018 wurden knapp 15.000 Handys ausgelesen; in den Asylverfahren tatsächlich verwendet wurde nur jeder dritte Datensatz. Von diesen 5.000 digitalen Infopaketen bestätigten laut Bundesinnenministerium ein Drittel die Angaben der Flüchtlinge. Lediglich in zwei Prozent, also in rund 100 Fällen, ergaben sich Widersprüche. Unbekannt ist allerdings, ob sich diese Widersprüche im Gespräch mit den Antragstellern auflösen ließen oder auf diese Weise Lügen enttarnt wurden. Laut Innenministerium für die Bundesregierung lasse sich dies statistisch nicht ermitteln. Es flössen „viele andere Aspekte" in die Bewertung ein: „Auch wenn die ausgelesenen Daten gegen die angegebene Herkunft sprechen, kann es im Einzelfall sein, dass es andere Erkenntnisse gibt, die letztlich zu einer Bestätigung der Herkunftsangabe führen." Sicher aber ist, dass das Gros der ausgewerteten Handys, knapp zwei Drittel, also rund 10.000, zu Identität und Herkunft „keinen relevanten Informationsgehalt erkennen" ließen.

Für Ulla Jelpke, innenpolitische Sprecherin der Linken, widerlegen die Auswertungen „ein verbreitetes Vorurteil: Ein Missbrauch oder falsche Angaben von Asylsuchenden in einer relevanten Größenordnung lassen sich damit gerade nicht belegen". Die Zahlen „unterstreichen die Unverhältnismäßigkeit dieser massenhaften Verletzung des Rechts auf informelle Selbstbestimmung" (Kastner, Flüchtlinge Auswertung von Handys bringt kaum Nutzen, www.sueddeutsche.de 08.07.2018).

Bund

Online-Zugriffe auf AZR sollen Regelfall werden

Im Koalitionsvertrag zwischen den Unionsparteien und der SPD ist vorgesehen, dass das Ausländerzentralregister (AZR) so modifiziert wird, dass künftig alle „relevanten Behörden ... belastbare Auskünfte" erhalten können. Bisher müssen Auskunftsersuchen in vielen Fällen schriftlich an das Bundesverwaltungsamt (BVA) gerichtet werden, was gemäß dem Bundesinnenministerium (BMI) zu „Verzögerungen in Verwaltungsabläufen" führt. Das BMI arbeitet an einem Gesetzentwurf, der den Datenabruf im automatisierten Verfahren für alle öffentlichen Stellen zum Regelfall machen soll. Auch Gerichte sollen Daten in Echtzeit abrufen können. Eine Sprecherin: „Das AZR ist hinsichtlich seiner Nutzungsmöglichkeiten ausbaufähig." Die Vorsitzende Richterin am Verwaltungsgericht Köln Rita Zimmermann-Rohde weist jedoch darauf hin, dass es nicht Aufgabe der Gerichte sein könne, nachzuprüfen, ob sich ein Verfahrensbeteiligter noch im Land befinde oder bereits abgeschoben worden sei. Es sei vielmehr „lege artis", dass die zuständigen Behörden die Gerichte entsprechend informierten (Digitale Kooperation, Der Spiegel Nr. 30, 21.07.2018, 12).

Bund

Gesundheitsminister Spahn will Smartphone-Zugriff auf Patientendaten

Gesetzlich Krankenversicherte sollen gemäß den Vorstellungen von Bundesgesundheitsminister Jens Spahn spätestens 2021 ihre Patientenakte auch auf dem Handy einsehen können: „Versicherte sollen auch per Tablet und Smartphone auf ihre elektronische Patientenakte zugreifen können". Das sei nicht das Ende der elektronischen Gesundheitskarte, aber eine zusätzliche, patientenfreundliche Option. Diese Pläne stoßen auf Kritik: Eine Weitergabe

von Patientendaten an Krankenkassen, Arbeitgeber und andere Dritte müsse ausgeschlossen sein, forderte der Ärzteverband Marburger Bund. Er unterstützt zwar, dass digitale Neuerungen für alle PatientInnen verfügbar gemacht werden sollen. Bei der beschleunigten Einführung elektronischer Patientenakten müsse jedoch der Datenschutz eingehalten werden. Zentral sind für den Ärzteverband dabei ein geschütztes Kommunikationsnetz und einheitliche Standards. Bei der Sicherheit dürfte es keine Abstriche geben. Das Arztgeheimnis dürfe nicht in Gefahr geraten. Das informationelle Selbstbestimmungsrecht der PatientInnen dürfe nicht untergraben werden.

Zudem verlangt der Marburger Bund, dass die Nutzung elektronischer Akten für PatientInnen freiwillig sein wird. Ob Daten gespeichert werden, müsse jeder selbst entscheiden. Ärztliche Beratung sei dabei zentral. Denn gerade ältere oder mehrfach erkrankte PatientInnen könnten zwar am meisten von der elektronischen Patientenakte profitieren – doch gerade sie seien oft nicht in der Lage, ihre Akte ganz allein zu verwalten.

In eine ähnliche Richtung geht die Kritik des Vereins Patientenrechte und Datenschutz e. V. Dr. Bernhard Scheffold, Physiker und Software-Entwickler, erklärte für den Verein: „Gesundheits- und Behandlungsdaten auch noch online zugänglich zu machen und damit für das Internet zu öffnen, wäre ein inakzeptables Sicherheitsrisiko, weil damit eine Vielzahl von Angriffs- und Zugriffsmöglichkeiten für Hacker, Geheimdienste und andere an diesen Daten interessierten Organisationen geschaffen würden.“ Uta Schmitt vom gleichen Verein ergänzt: „Aus unserer Sicht müssen folgende grundlegende Rechte und Freiheiten der gesetzlich Versicherten dauerhaft rechtlich und tatsächlich gesichert werden: das Recht auf Vertraulichkeit (Arztgeheimnis), das Recht auf strikte Beachtung der Zweckbindung der Patientendaten, das Recht auf freie Arztwahl, das Recht, keine elektronische Gesundheitsakte zu haben, das Recht auf volle Verfügung über die eigene Akte. Die zur Wahrung dieser Patientenrechte erforderlichen rechtlichen, technischen und organisatorischen Rahmenbedingungen sind zu erhalten bzw. neu zu schaffen. Was Herr Spahn fordert, widerspricht diesen Grundsätzen.“

Die von Spahn angedachte Smartphone-Version der elektronischen Patientenakte werde lediglich die Kosten für Versicherte und ihre Krankenkassen deutlich in die Höhe treiben. Dies sei angesichts der bisher für die Entwicklung der elektronischen Gesundheitskarte (eGK) aufgelaufenen Kosten von mehr als zwei Milliarden Euro unverantwortlich (Ärzte fordern Sicherheit für digitale Krankenakte, SZ 24.07.2018, 5; PM Patientenrechte und Datenschutz e.V., Das ist #Spahnsinn! 23.07.2018).

Bundesweit

Private und öffentliche Krankenversicherer bieten E-Gesundheitsakte an

Nach AOK und Technikerkrankenkasse (TK) stellte erstmals ein Konsortium von gesetzlichen und privaten Krankenversicherern gemeinsam eine elektronische (E-) Gesundheitsakte vor, mit der die Versicherten über eine App alle ihre Gesundheitsdaten verwalten können sollen. Die am 05.06.2018 in Berlin vorgestellte E-Gesundheitsakte „Vivy“ sollen zunächst 25 Millionen Versicherte nutzen können, die Mitglied bei einer der beteiligten Krankenkassen und Unternehmen sind. Dazu gehören unter anderen Betriebs-, Ersatz- und Innungskrankenkassen, u. a. die DAK Gesundheit, die Bahn BKK und die ikk classic sowie die Krankenversicherer Allianz, Gothaer, Süddeutsche und Barmenia. Daniel Bahr, Vorstand der Allianz Private Krankenversicherung und einst FDP-Gesundheitsminister, erklärte: „Es gibt viele weitere, die Interesse haben.“ Die vom Berliner Start-up Vivy entwickelte systemübergreifende Lösung wird von Bitmarck unterstützt, dem IT-Dienstleister von mehr als 90 Krankenkassen sowie mehreren privaten Krankenversicherungen. Die Allianz SE ist mit 70% an der Vivy GmbH beteiligt. Die restlichen 30% hält der Gründer und Geschäftsführer Christian Rebernik.

Ziel ist es, mit dem digitalen Angebot Versicherten die Möglichkeit zu geben, ihre persönlichen Gesundheitsdaten in einer App zu verwalten. Darüber hinaus hat Vivy gemäß einer Mitteilung den Anspruch, Nutzenden jederzeit als digitale Gesundheitsassistentin zur Seite zu stehen. Die Versicherten hätten dabei die volle Kontrolle über ihre Daten; nur sie selbst entscheiden, welche Informationen sie in der App speichern und an wen sie diese weitergeben möchten. Erfasst werden können über die Vivy-App „einfach und sicher“ Arztbriefe, Befunde, Laborwerte, Medikationspläne, Notfalldaten und Impfinformationen. Die Anwendung soll möglichst einfach zu handhaben sein, auch bei der Anbindung an die Arzt- und an die Kliniksoftware. Die Ärzteschaft soll Untersuchungsdaten sehr einfach in der Vivy-App ihrer PatientInnen bereitstellen können, sie müssten dafür keine extra Software installieren.

Die Nutzenden sollen dann über Vivy ihre Patientendaten bei den behandelnden Arztpraxen abfragen können, welche die Daten auf dem vorgegebenen digitalen Weg bereitstellen. Bei dieser Datenabfrage handele es sich grundsätzlich nicht um eine Weiterleitung von personenbezogenen Daten an Dritte, sondern um eine Datenabfrage des Patienten als betroffene Person im Sinne der Datenschutzgrundverordnung (DSGVO). Bahr: „Als Versicherer können wir die Daten nicht sehen.“ Die Akte soll für Versicherte freiwillig und kostenlos sein. Schon im Juli 2018 begannen die ersten Krankenkassen, ihre Versicherten in die Vivy-App einzuladen.

Hintergrund des neuen Angebots ist, dass die Entwicklung der elektronischen Gesundheitskarte (eGK) im Rahmen der offiziellen Telematik-Infrastruktur und damit auch eine bundesweit einheitliche elektronische Patientenakte weiterhin nur schleppend vorankommt. Vor dem Konsortium waren schon die AOK und der TK mit eigenen Angeboten vorgeprescht. Bahr betonte, dass sie keine weitere Insellösung wollen. Je mehr unterschiedliche Angebote bestehen, umso schwieriger werde die Anbindung für die Ärzteschaft und die Krankenhäuser (Digitale Gesundheitsplattform für 25 Millionen Versicherte, www.aerzte-zeitung.de 05.06.2018; Schlingensiepen, Gesundheitsakte für 25 Millionen, SZ 06.06.2018, 19).

Bundesweit

DSGVO-Abmahnungen sind unterwegs

Die Befürchtungen, dass mit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) eine Abmahnwelle starten würde, haben sich nicht bestätigt. Letztlich ist es ziemlich ruhig geblieben. Auch Abmahn-Anwälten scheint oft nicht so richtig klar zu sein, was jetzt erlaubt ist und was verboten. Einige sind dennoch tätig geworden und haben für ihr Tätigwerden Mandanten erfunden. Diese Masche zeigte sich beispielsweise bei einer Zeitarbeitsfirma aus Nordrhein-Westfalen, die Tischler vermittelt. Bei „Tischler für NRW" trudelten Anfragen von erbosten Konkurrenten ein, die dem Anschein nach im Auftrag der Firma von einer Kanzlei abgemahnt wurden. Das entsprach aber nicht der Wahrheit, wie das Unternehmen dann auch groß und breit auf der offiziellen Homepage erklärte. Demnach existierte kein Auftrag für solche Abmahnungen und die Kanzlei besaß auch keine Vollmacht.

Auch die Ärzteschaft wird mit Abmahnungen traktiert. Viele ÄrztInnen wurden aufgefordert, binnen kurzer Zeit die Anwaltsgebühren zu zahlen, ansonsten drohten Zwangsmaßnahmen, weitere juristische Schritte und möglicherweise ein Prozess. Hintergrund der Abmahnungen sind jeweils die Homepages, auf denen gemäß der DSGVO die Datenschutzerklärungen angepasst werden müssen. Es wird empfohlen, in solchen Fällen die Webseiten kurzzeitig vom Netz zu nehmen, bis alles den neuen DSGVO-Regeln entspricht. Es sollte Kontakt mit dem angeblichen Auftraggeber der Abmahnung aufgenommen werden, um festzustellen, ob tatsächlich ein Auftrag von einem Konkurrenzunternehmen besteht. Möglicherweise handelt es sich bei den Schreiben um Betrug. Statt sofort zu zahlen, sollte im Zweifelsfall, so die Empfehlung des Hamburgischen Datenschutzbeauftragten, ein Anwalt eingeschaltet werden (Michelsen, DSGVO-Abmahnungen: Abzock-Kanzleien erfinden Kunden, www.computerbild.de 08.06.2018; Hamburger Ärzte empört über Abmahnbriefe, Hamburger Abendblatt 20.07.2018).

Bundesweit

Datenschutzaufsichtsbehörden mit DSGVO überfordert

Der erste Monat mit der neuen europäischen Datenschutz-Grundverordnung (DSGVO) hat die zuständigen deutschen Aufsichtsbehörden weit über ihre Leistungsgrenzen gefordert. Im Juni 2018 sind in vielen Bundesländern bereits mehr Beschwerden eingegangen als zuvor innerhalb eines Jahres. Neben Beschwerden bekommen die Landes-Datenschützer auch viele Nachfragen von Unternehmen und Bürgern zum Umgang mit den neuen, seit dem 25.05.2018 wirksamen Regeln.

In Baden-Württemberg landeten allein über das entsprechende Online-Formular auf der Internetseite der Datenschützer im ersten Monat 211 Beschwerden; den Monat zuvor waren es nur 66.Von einer Verdreifachung ist auch in Hessen die Rede. Seit Ende Mai verzeichnete man dort bislang 450 Beschwerden. Eine Sprecherin des hessischen Datenschutzbeauftragten Michael Ronellenfitsch erläuterte: „Wir nennen uns nur noch Call-Center. Die Zahl der Anfragen ist extrem hoch. Vor allem bei Firmen, Kommunen und auch bei Vereinen herrschen große Unsicherheiten." Auch Privatleute wenden sich mit ihren Fragen an die Behörde. Die nach zwei Jahren Übergangsfrist direkt anwendbare DSGVO, die den Datenschutz in Europa vereinheitlichen und den Kontrolleuren mehr Macht geben soll, hat jede Menge Verunsicherung ausgelöst.

Auch die DatenschützerInnen in Nordrhein-Westfalen versinken, so ein Sprecher, in einer Flut von Anfragen: „Die Telefone stehen nicht mehr still." Täglich nehme der mit nur einer Person besetzte Empfang rund 100 Anrufe zum Thema DSGVO entgegen. In den Tagen rund um den Start der neuen EU-Regeln am 25.05. seien es sogar 140 Anrufe täglich gewesen. Seit Anfang des Jahres bis Juni erreichten die NRW-DatenschützerInnen 4.700 schriftliche Eingaben – im gesamten Vorjahr waren es nur knapp 4.000. Allerdings fallen darunter nicht nur Beschwerden, sondern auch Beratungsanfragen.

Besonders viele Beschwerden gingen ein, direkt nachdem die neue Verordnung wirksam wurde. In Berlin beispielsweise waren es allein am 28. Mai rund 130 Beschwerden. Das entspricht laut der zuständigen Landesbehörde einem zehn Mal höheren Aufkommen als vor Beginn der DSGVO-Ära. Mittlerweile habe sich die Zahl bei etwa 30 Beschwerden pro Tag eingependelt, heißt es – was immer noch das Dreifache der ursprünglichen Menge sei. Als Schwerpunkte kristallisierten sich Online-Handel und Lieferdienste für Essen heraus. Die Fälle werden nun geprüft und die Unternehmen um Stellungnahme gebeten. Viele BürgerInnen seien im Zuge der Berichterstattung über die neuen Regeln stärker in Sachen Datenschutz sensibilisiert: „Sie haben davon erfahren, dass es Datenschutz überhaupt gibt, das war vorher bei vielen nicht bekannt." Die DSGVO soll Menschen mehr Mitsprache dabei geben, was mit ihren Daten in Unternehmen, Vereinen oder Behörden passiert. Beim Hamburger Datenschutzbeauftragten Johannes Caspar gingen fast doppelt so viele Beschwerden wie zuvor ein. Insgesamt wandten sich im ersten DSGVO-Monat 460 Mal BürgerInnen an die Behörde. 260 dieser Eingänge wurden bereits ausgewertet. In 60% der Fälle beschwerten sich die Menschen über Verstöße gegen die neue DSGVO.

In Schleswig-Holstein gingen rund 400 Beschwerden ein. Einige davon richteten sich gemäß der Landes-Datenschutzbeauftragten Marit Hansen zugleich gegen mehrere Verantwortliche: „Beispielsweise ging es in einer Beschwerde um mehr als 20 mutmaßliche Datenschutzverstöße." Manchmal reichten für denselben Fall mehrere Betroffene Beschwerde ein. In einem Fall habe es vier getrennte Beschwerden gegeben. Die Betroffenen haben gemäß der DSGVO grds. einen Anspruch auf Antwort innerhalb von einem Monat.

Dieter Kugelmann, Landesdatenschutzbeauftrager in Rheinland-Pfalz, erklärte, dass Verbraucherinnen mit ihren Beschwerden vor allem auf vermeintliche Missstände in sozialen Netzwerken wie Facebook aufmerksam machen: „Aber auch wegen Videokameras in Geschäften, Straßen oder beim Nachbarn melden sich viele Menschen."

Bei Kugelmann liefen im Juni 2018 insgesamt 123 Beschwerden auf.

In Thüringen dagegen gab es nach Angaben des Datenschutzbeauftragten Lutz Hasse keinen signifikanten Anstieg von Beschwerden im Zusammenhang mit der Datenschutzgrundverordnung. „Allerdings haben sich die Eingangszahlen auf bis zu 500 pro Tag deshalb stark erhöht, weil sehr viele Fragen – auch von Unternehmen – zur DSGVO gestellt werden. Das ist sehr schön, drückt unsere Behörde aber kapazitätsmäßig ganz schön in die Knie" (DSGVO: Neue Regeln halten Datenschutz-Behörden in Atem, www.heise.de 23.06.2018; Datenschutz: 400 Beschwerden, Kieler Nachrichten 25.06.2018, 24; Seibel, Zahl der Datenschutz-Beschwerden explodiert, www.welt.de 01.07.2018).

Bundesweit

Polizei sammelt rechtsextreme „Feindeslisten"

Sicherheitsbehörden haben seit 2011 anlässlich von Razzien und Festnahmen bei gewaltbereiten Gruppen sogenannte „Feindeslisten" gefunden. Darauf sind die Daten von 25.000 Personen mit Namen, Telefonnummer und Adressen vermerkt. Dies ergaben journalistische Recherchen auf der Grundlage einer Antwort der Bundesregierung auf eine parlamentarische Anfrage der Linken.

Die entsprechenden Schriftstücke oder Datensätze stammen vor allem aus den Ermittlungen gegen den rechtsterroristischen Nationalsozialistischen Untergrund (NSU) bis Ende 2011 und aus den Ermittlungen gegen den terrorverdächtigen Bundeswehrsoldaten Franco A. und zwei Komplizen. Zahlreiche entsprechende Daten fanden sich auch bei den Ermittlungen gegen die rechte Prepper-Gruppierung „Nordkreuz" im Jahr 2017. Mit Prepper bezeichnet man Personen, die sich auf Katastrophen vorbereiten. Dazu lagern sie Lebensmittel ein, errichten Schutzbauten und lagern Schutzkleidung, Werkzeuge, Funkgeräte und Waffen ein.

Aus der Antwort der Bundesregierung geht hervor, dass es keine gemeinsame Datei von Bund und Ländern über bedrohte Personen auf diesen „Feindeslisten" gibt. Martina Renner von der Linkenfraktion im Bundestag warf der Bundesregierung vor, die rechtsterroristische Gefahr zu ignorieren: „Anders ist es nicht zu erklären, dass das Bundeskriminalamt von mehreren Zehntausend Betroffenen nicht mal eine Handvoll informiert und sich sonst ausschweigt" (Rechtsextreme setzten Tausende auf „Feindesliste", www.dw.com 30.07.2018).

Bundesweit

Vorerst nur in Bayern Regelanfragen bei Besetzung von Richterstellen

Auf Initiative von Hessens Justizministerin Eva Kühne-Hörmann (CDU) berieten die JustizministerInnen der Länder am 06./07.06.2018 über die Einführung einer Regelanfrage beim Verfassungsschutz bei der Einstellung von RichterInnen. Kühne-Hörmann meinte, man müsse Vorkehrungen treffen, um „die staatlichen Strukturen vor extremistischem Gedankengut zu bewahren", weil etwa durch den „Pakt für den Rechtsstaat" Personal in großem Umfang eingestellt werden solle. Sie orientiert sich dabei an Bayern, das die Regelanfrage seit Ende 2016 praktiziert. Mit „Einwilligung" der Bewerbenden wird beim Verfassungsschutz eine Regelanfrage durchgeführt. Es gelte, Mitglieder rechts- oder linksextremer wie auch islamistischer Gruppen auszufiltern. Damit sei kein Generalverdacht gegen potenzielle RichterInnen verbunden.

Der Antrag fand auf der JustizministerInnenkonferenz keine Mehrheit. Vielmehr wurde ein Beschluss gefällt, der mit Sorge zur Kenntnis nimmt, dass sich in jüngster Zeit vermehrt Menschen als RichterInnen bewerben, die „mit extremistischem, antidemokratischem und verfassungsfeindlichem Gedankengut in Erscheinung getreten sind". Es blieb bei einem Austausch über Möglichkeiten und Maßnahmen, insofern aktiv zu werden. Hamburgs Justizsenator Till Steffen (Grüne) erklärte, Hessen falle mit seinem Antrag „in antiliberale Verhältnisse der Siebzigerjahre zurück", also in Zeiten des „Radikalenerlasses" von 1972, der zu einer millionenfachen Überprüfung von Bewerbenden im öffentlichen Dienst geführt hatte und zu Berufsverboten, deren Folgen bis heute in den Rentenbiografien verhinderter Lehrer spürbar sind. Gemäß Steffen zieht eine Regelanfrage die Verfassungstreue von Bewerbenden grundsätzlich in Zweifel wegen weniger kritischer Fälle, in denen man meist auch ohne Verfassungsschutzämter Erkenntnisse habe.

Auch der Vorsitzender der Konferenz Thüringens Justizminister Dieter Lauinger (Grüne), stimmte gegen den Vorschlag. In Thüringen werde auch ohne Regelanfrage keinE KandidatIn nur aufgrund der Examensnote eingestellt. Diese würden intensiv von Fachgremien befragt. Ähnlich hält man es in Rheinland-Pfalz; wo die Verfassungsschutzbehörde bei Zweifeln über die Verfassungstreue eingeschaltet wird. Auch Bremens Justizsenator Martin Günthner (SPD) votierte gegen eine Regelanfrage und wies darauf hin, dass die Zustimmung von den Bewerbern ja nicht wirklich freiwillig erteilt werde.

Das bayerische Landesamt für Verfassungsschutz gibt an, nur „gerichtsverwertbare Tatsachen" weiterzugeben. Das könne „Reichsbürger", Islamisten und autonome Linksextremisten betreffen oder auch AfD-Mitglieder, die wegen enger Kontakte zur rechtsextremen Szene unter Beobachtung des Verfassungsschutzes stünden. Die Partei selbst werde nicht beobachtet. Informationen von V-Leuten seien nicht gerichtsverwertbar, selbst dann nicht, wenn sie einen Richteramtsbewerber bei einem rechtsextremen Liederabend gesehen hätten. Seit Einführung der Regelanfrage im November 2016 gab es in Bayern keinen einzigen Treffer, sondern nur Fehlanzeigen (Janisch, Richter sollen auf ihre Gesinnung geprüft werden, SZ 05.06.2018, 89. Konferenz der Justizministerinnen und Justizminister 6./7.6.2018, Beschluss TOP I.16).

Bayern

Verfassungsklagen gegen PAG

Die Landtagsfraktion der Grünen, die fraktionslose Abgeordnete Claudia Stamm der Partei „mut" sowie die SPD-

Fraktion wollen über eine richterliche Prüfung klären lassen, ob das von der CSU-Mehrheit gegen die Stimmen der gesamten Opposition verabschiedete und am 25.05.2018 in Kraft getretene Polizeiaufgabengesetz (PAG) die Freiheitsrechte der BürgerInnen übermäßig einschränkt und deshalb verfassungswidrig ist (vgl. DANA 1/2018, 11 ff.). Folgen könnten noch Linke und FDP, die erklärt haben, dass sie auch klagen wollen.

SPD-Landeschefin Natascha Kohnen begründete den Schritt: „Wir verteidigen den Freistaat Bayern gegen das illiberale Gesetz der CSU“. Nach ihrer Auffassung beschneidet das Gesetz „die Freiheit der Bürgerinnen und Bürger in einer für unsere Demokratie unerträglichen Weise und begegnet ihnen mit tiefem Misstrauen.“ Gemäß dem neuen PAG genügt schon eine drohende Gefahr, um Überwachung und andere polizeiliche Maßnahmen, etwa DNA-Tests, einzuleiten. Die SPD zieht nicht nur vor den bayerischen Verfassungsgerichtshof, sondern wählt, wie Claudia Stamm, auch noch den Weg vor das Bundesverfassungsgericht. Dies sei nötig, da die CSU das Gesetz zum Muster für alle Landesgesetze machen wolle. Der Polizeirechtler Mark Zöller hat in seiner Klageschrift für die SPD-Fraktion eine Mängelliste von 20 Verfassungsverstößen aufgeführt. Zöller: „Da haben Überwachungsfantasten ihre Wunschträume verwirklicht. Bei der Überwachung von Wohnungen erfülle das Gesetz die Vorgaben des Grundgesetzes nicht. Fußballfans hätten zu Recht moniert, dass man sie mit Übersichtsaufnahmen von Drohnen anlasslos überwache. Durch den Rechtsbegriff der „drohenden Gefahr“ könne die Polizei schon bei „Verdacht, demnächst einen Verdacht“ zu haben, eingreifen. Er sei zu schwammig und verstoße damit gegen das verfassungsrechtliche Bestimmtheitsgebot.

Die Grünen haben am 06.06.2018 beim Bayerischen Verfassungsgerichtshof Klage eingereicht. Einen überdimensionalen Briefumschlag, in dem angeblich die Klageschrift steckte, hatte Katharina Schulze, Fraktionsvorsitzende der Grünen im Landtag, gebastelt. Von der ebenso groß geratenen Briefmarke stierten zwei Überwachungskameras herunter. Schulze meinte, das neue PAG sei vom „Überwachungswahn der CSU“ geprägt. Der Staatsrechtler Christoph Degenhart von der Universität Leipzig hat die Klage für die Grünen verfasst. Die Balance von Freiheit und Sicherheit werde nicht gewahrt. Eingriffe in die Grundrechte der BürgerInnen seien für 39 Maßnahmen bei „drohender Gefahr“ erlaubt.“ Die Polizei könne jetzt früher Telefone abhören oder E-Mails lesen. Betroffen sei jedermann. Das Bundesverfassungsgericht verwende die „drohende Gefahr“ dagegen nur in Zusammenhang mit Terrorismus. Stören müssten das Gericht nach Meinung Deegenharts auch geplante Übersichtsaufnahmen bei Menschenansammlungen. Da die Technik es erlaube, den Einzelnen hervorzuheben, sieht er einen Eingriff in die Grundrechte.

Die Landesregierung hält dem entgegen, die Polizei soll gemäß dem Gesetz viele Eingriffe künftig bei einem Richter beantragen. Nur in Einzelfällen dürften Polizeibeamte selbst entscheiden. Um die rechtsstaatliche Anwendung zu wahren, solle über die Umsetzung des Gesetzes soll eine Kommission unter Vorsitz des Verfassungsrechtlers Karl Huber wachen.

Der frühere Ministerpräsident Horst Seehofer, unter dem das Gesetz geschrieben wurde, sieht das Gesetz als Vorbild für die neuen Polizeiaufgabengesetze aller Bundesländer. Die Opposition wirft der CSU dagegen vor, das Gesetz unter Missachtung des Bürgerwillens durchgebracht zu haben. Auch die zum bürgerlich-konservativen Lager zählenden Freien Wähler sind kritisch. Bei einer Demonstration gingen am 10.05.2018 in München über 30.000 vor allem junge Menschen gegen das neue Polizeirecht auf die Straße. Die Gewerkschaft der Polizei (GdP) äußerte Zweifel an der Akzeptanz des Gesetzes in der Bevölkerung (SPD klagt ebenfalls gegen Polizeigesetz, SZ 08.06.2018, 40; Grüne klagen gegen neues Polizeiaufgabengesetz, www.sueddeutsche.de 06.06.2018; Bayern-SPD klagt gegen Polizeigesetz, www.zeit.de 24.05.2018).

Hessen

Schufa-Auskunftsverfahren in Konflikt mit DSGVO

Die Schufa, die Schutzgemeinschaft für allgemeine Kreidtsicherung mit Sitz in Wiesbaden, verfügt nach eigenen Angaben in Deutschland über Daten von rund 67,5 Millionen Menschen. Diese Daten sollen Auskunft geben über deren Bonität, also der Zahlungsfähigkeit und -bereitschaft. Wer eine kreditorische Vertragsbeziehung eingehen, z. B. einen Mietvertrag abschließen möchte, von dem wird oft eine Schufa-Selbstauskunft abverlangt. Um diese schnell zu bekommen, muss der Betroffene zahlen. Das Angebot „Meine Schufa“ kostet monatlich 3,95 Euro und läuft mindestens ein Jahr. Zwar besteht gemäß dem Datenschutzrecht schon bisher ein Anspruch auf kostenfreie Auskunft, doch lässt sich die Schufa damit Zeit. Es dauert etwa zwei Wochen, bis diese den Weg per Post in den eigenen Briefkasten findet, was für einen Vertragsabschluss zu spät sein kann.

Dem für die Schufa zuständigen hessischen Datenschutzbeauftragten (HDSB) stört diese Verzögerung. Gemäß der seit Ende Mai geltenden Datenschutzgrundverordnung (DSGVO) müssen Unternehmen zeitnah und auf elektronischem Weg Auskunft erteilen, wenn die Anfrage der Person auch auf diesem Weg erfolgt ist. Hat die Person die Auskunft elektronisch beantragt, sollen die Unternehmen – sofern nicht anders angegeben – auch auf diesem Wege antworten. Art. 15 DSGVO sieht vor, dass VerbraucherInnen kostenlos und „unverzüglich“ eine Kopie der über sie gespeicherten personenbezogenen Daten bekommen können. „Unverzüglich“ bedeutet gemäß Art. 12 Abs. 3 DSGVO aber, dass es bis zur Auskunft einen Monat dauern kann; in komplexen Ausnahmefällen darf die Frist um bis zu zwei Monate verlängert werden.

Die kostenfreie Kopie nach Artikel 15 DSGVO lässt sich über die Website der Schufa zwar bestellen, auch wenn man sich erst einmal eine Weile durch das Dickicht der kostenpflichtigen Angebote klicken muss. Allerdings bekommt man diese nur per Post zugesandt. Laut Schufa ist dieses Vorgehen mit der Aufsichtsbehörde, dem HDSB, abgestimmt. Der Weg per Brief sei zulässig. Da die Anschriften der Betroffenen ohnehin bei der Schufa gespeichert seien, sei so eine Identifizierung und sichere Zustellung an den berechtigten Auskunftsempfänger möglich. Zudem habe die

Schufa in der Regel keine verifizierten elektronischen Kontaktmöglichkeiten wie E-Mail-Adressen der jeweiligen Betroffenen.

Beim kostenpflichtigen Angebot „Meine Schufa" wird die Auskunft dagegen auch Online erteilt. Die Identität der Anfragenden wird dort über die Prüfziffern des Personalausweises sichergestellt. Dieser Onlinezugang sei allerdings, so argumentiert die Schufa, auch nicht sofort, sondern erst nach einer Prüfung verfügbar. Nach dem Identverfahren mittels Personalausweis werden die Zugangsdaten per Post zugesendet. Das dauere dann etwa so lang wie die Postzustellung der DSGVO-Datenkopie.

Die Schufa findet den Vergleich zwischen den eigenen kostenpflichtigen Angeboten und der kostenlosen DSGVO-Auskunft nicht für zulässig. Dabei handele es sich um komplett verschiedene Angebote. Die Schufa sei wie jedes andere Unternehmen frei in der Gestaltung seiner Angebote. Außerdem sei die DSGVO-Kopie auch nur für den Betroffenen selbst gedacht und ausdrücklich nicht für die Weitergabe an Dritte, zum Beispiel an den künftigen Vermieter. Die Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) erklärte hierzu, dass dies aus Datenschutzgründen sinnvoll sei, da die DSGVO-Selbstauskunft häufig mehr Angaben über die wirtschaftlichen Verhältnisse enthält, als für eine Beurteilung der Bonität im Rahmen eines Mietverhältnisses erforderlich sei (Hauck, Schufa auf dem Prüfstand, SZ 12.06.2018, 20).

Nordrhein-Westfalen

Neues Terrorabwehrzentrum

Als Reaktion auf das Anis-Amri-Attentat in Berlin ordnet der Innenminister von Nordrhein-Westfalen (NRW) Herbert Reul (CDU) den Staatsschutz seines Landes neu. Gemäß einem Erlass soll im Landeskriminalamt (LKA) zum 01.01.2019 eine Abteilung Terrorismusbekämpfung eingerichtet werden, die sich mit den etwa 20 als gefährlich eingestuften Islamisten im Lande befasst. Bislang wurden in NRW die Fälle aller 272 islamistischen Gefährder dezentral in den Polizeibehörden der Wohnorte bearbeitet. Innerhalb der neuen LKA-Abteilung soll ein Terrorismusabwehrzentrum entstehen, ähnlich zum Gemeinsamen Terrorismusabwehrzentrum (GTAZ) auf Bundesebene in Berlin. In diesem neuen Zentrum sollen Beamte von ihren örtlichen Dienststellen entsandt werden. Die hohe Gefährdungslage mache, so der Erlass, eine Neuorganisation des Staatsschutzes und die Konzentration der Kräfte notwendig. Zuvor hatte schon das Bundeskriminalamt angekündigt, eine eigene Abteilung für islamistischen Terrorismus zu gründen. Die Zahl der Ermittlungsverfahren in dem Bereich hat sich in den vergangenen Jahren vervielfacht (NRW gründet eigenes Terrorabwehrzentrum, Der Spiegel Nr. 30, 21.07.2018, 11).

Nordrhein-Westfalen

Kita schwärzt Fotos von Kindergesichtern

Eine Kindertagesstätte in Hackenbroich in Nordrhein-Westfalen machte im Juli 2018 aus Datenschutzgründen Kinder in Fotomappen für die AbgängerInnen nachträglich unkenntlich. Die Gesichter auf den Fotos wurden mit Filzstift übermalt. Die Gesichter der Kinder der katholischen Kindertagesstätte St. Michael wurden in den Erinnerungsalben, die ihnen die Betreuerinnen zusammengestellt und zum Abschied übergeben haben, mit schwarzem Edding überkritzelt. Der Grund war die Angst vor einem Verstoß gegen die Datenschutzverordnung. Die Leitung der Kindertagesstätte ließ sämtliche Personen unkenntlich machen; verschont blieb jeweils nur das Kind, dem die Mappe gehörte.

Die Empörung der Eltern war groß. Nachdem die lokale Presse über den Vorfall berichtete und die Geschichte bundesweit von den Medien aufgegriffen wurde, stand im Kindergarten St. Michael das Telefon nicht mehr still. Dort wollte man sich deshalb nicht mehr dazu äußern und verweist stattdessen auf das zuständige Pastoralbüro in Dormagen. Pfarrer Peter Stelten erklärte, es sei ihm bewusst, dass eine solche Erinnerungsmappe nicht schön sei: „Aber wir brauchten eine wasserdichte Lösung, also haben wir uns für den sicheren Weg entschieden." Die Alternative wäre gar keine Mappe gewesen. „Es musste flott gehen, wegen des neuen kirchlichen Datenschutzgesetzes". Dieses trat am 25.05.2018 in Kraft.

Die Konferenz der Diözesanbeauftragten hatte einige Zeit zuvor einen Leitfaden herausgegeben, mit dessen Hilfe sich Einrichtungen auf die Neuerungen in Sachen Datenschutz vorbereiten konnten. Stelten erläuterte: „In einem Alltag, wo jede freie Hand für die Kinder gebraucht wird, konnten wir uns damit nicht ausführlich genug auseinandersetzen". Dafür sei das Thema viel zu komplex. Nele Trenner, eine Anwältin, die sich auf Datenschutz bei Kindern spezialisiert hat, zeigte hierfür Verständnis: „Im normalen Alltag kann man solche Vorgaben kaum noch ohne juristischen Sachverstand lösen." Natürlich sei es absurd, eine Erinnerung im Nachhinein zu schwärzen, statt zuvor die Erlaubnis der Eltern einzuholen. Solche Maßnahmen seien aber in Wirklichkeit weniger ein Anlass für Spott als ein Zeichen für ein tiefergehendes Problem: die kollektive Rat- und Hilflosigkeit, wie sie schon länger im Umgang mit persönlichkeitsbezogenen Daten von Privatpersonen existiere. Das entsprechende Gesetz sei zwar zum Schutz von Privatpersonen gemacht worden, könne aber nicht von ihnen durchschaut und genutzt werden.

Es ist kein Wunder, dass Einrichtungen für Kinder besonders vorsichtig sind und alles richtig machen wollen. Zwar sei es, so Trenner, üblich, dass Eltern im Vorhinein schriftlich erklären, ob Fotos von ihren Kindern gemacht und in Mitgliederzeitschriften oder im Internet veröffentlicht werden dürfen. Allerdings komme es vor, dass Eltern diese Erklärung später widerrufen mit dem Argument, dass diese nicht freiwillig erfolgt sei, etwa wenn die Einverständniserklärung in die Anmeldung zum Kindergarten integriert ist, so wie es bei der Kindertagesstätte in Hackenbroich der Fall war: „Manche Eltern schrecken in so einem Moment vor einer Ablehnung zurück, weil sie fürchten, durch ihre Verweigerung die Zusage für den Kita-Platz zu riskieren". So gesehen habe der Träger in diesem Fall eindeutig richtig gehandelt. Dennoch sollte man sich

von den neuen Datenschutzregelungen nicht verrückt machen lassen. Es ist ja nicht so, dass jeder gleich verklagt werde: „Im Umgang mit solchen Gesetzen funktioniert tatsächlich noch vieles mit dem gesunden Menschenverstand."

Im neuen Jahr soll in St. Michael alles besser werden. Pfarrer Stelten erklärte, die Deutsche Bischofskonferenz sei gerade dabei, ein Regelwerk zu erarbeiten, das den Bedürfnissen aller gerecht werde. Für die nächste Generation der Vorschulkinder soll es dann Erinnerungsmappen geben, die man später gerne anschaut, weil auch die Gesichter zu erkennen sind (Simon, Geschwärzte Erinnerung, SZ 04./05.08.2018, 10).

Datenschutznachrichten aus dem Ausland

EU

5. Geldwäsche-Richtlinie tritt in Kraft

Der Rat der Europäischen Union (EU) hat am 15.05.2018 ohne weitere Aussprache die 5. Reform der Richtlinie gegen Geldwäsche und Terrorismusfinanzierung angenommen, mit der Kryptogeldkäufe aus der „Anonymität" geholt werden sollen. Einen Monat zuvor hatte das EU-Parlament den Regelungen zugestimmt.

Von der Richtlinie werden erstmals die Betreiber von Wechselstuben für virtuelle Währungen wie Bitcoin, Ethereum oder Ripple sowie Anbieter elektronischer Geldbörsen erfasst, die künftig ihre KundInnen im Rahmen der „üblichen Sorgfaltspflichten" für Finanzhäuser kontrollieren müssen. Die Umtausch-Plattformen für Kryptowährungen sollen gemäß den neuen Vorgaben die Identität der Nutzenden sowie deren Wallet-Adressen in einer zentralen Datenbank speichern. Parallel müssen sie es ermöglichen, dass Details über den Einsatz der Zahlungssysteme durch Selbstangaben der Nutzenden aufgezeichnet werden können. Ziel ist es, die angebliche Anonymität virtueller Währungen aufzuheben und das damit verbundene „Missbrauchspotenzial für kriminelle Zwecke" zu minimieren.

Alle Finanzinstitute müssen auf Basis der neuen Richtlinie insbesondere Belege zu sämtlichen Transaktionen fünf bis maximal zehn Jahre nach dem Ende der Geschäftsbeziehung aufbewahren. Da vor allem Bankkonten oft jahrzehntelang geführt werden, kann sich eine im Einzelfall nicht vorhersehbare Archivfrist ergeben. Im Idealfall sollen alle betroffenen Einrichtungen zudem ihre KundInnen identifizieren und die entsprechenden Daten genauso lange vorhalten wie die Transaktionsbelege.

Auf Abruf müssen die Verpflichteten ihre gesammelten Nutzerinformationen einer zentralen nationalen Analysestelle in Form der „Financial Intelligence Unit" (FIU) zur Verfügung stellen. Der Anwendungsbereich der Richtlinie bleibt vage. So gelten etwa auch alle einschlägigen Straftaten, die mit einer Höchststrafe von über einem Jahr belegt sind, bereits als Vortaten zur Geldwäsche. Erfasst werden können so selbst einfache Delikte wie üble Nachrede. KritikerInnen sehen in den Klauseln eine unverhältnismäßige Verpflichtung zur Vorratsdatenspeicherung und eine massive Einschränkung des Bankgeheimnisses.

Anonyme Zahlungen über Prepaid-Karten werden weiter eingeschränkt. Den bisherigen europäischen Schwellenbetrag von 250 Euro, für den keine Identitätsangabe nötig war, senkt der EU-Gesetzgeber auf 150 Euro; in Deutschland liegt das Limit derzeit schon bei 100 Euro. Auch bei Guthabenkarten sollen strengere Vorschriften zur Kundenüberprüfung gelten.

Der bulgarische Finanzminister Wladislaw Goranow begründete die Reform im Namen der Ratspräsidentschaft als Antwort auf das erhöhte Sicherheitsbedürfnis in Europa; mit ihr werde der Spielraum für Terroristen weiter eingeschränkt. Es werde möglich, kriminelle Netzwerke zu zerstören. Die Grundrechte und wirtschaftlichen Freiheiten blieben gewahrt. Die aktualisierte Richtlinie tritt nach Veröffentlichung im EU-Amtsblatt in Kraft. Die Mitgliedstaaten haben dann 18 Monate Zeit, diese in nationales Recht umzusetzen. Für einen Teil der Bestimmungen gelten längere Übergangsfristen. (Krempl, Geldwäsche: EU-Staaten besiegeln Finanzdatenspeicherung und Aus für anonymen Kryptogeldkauf, www.heise.de 17.05.2018).

Österreich

FPÖ versucht mit Handstreich Geheimdienst gleichzuschalten

Am 29.05.2018 veröffentlichte das Wiener Stadtmagazin „Falter" Mails aus dem Innenleben des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT), die den Verdacht erhärten, dass der Inlandsgeheimdienst gezielt sturmreif geschossen werden soll. Ende Februar 2018 kam es beim BVT und in vier Privatwohnungen zu Hausdurchsuchungen; wenig später wurde der Behördenleiter Peter Gridling vom neuen österreichischen Innenminister Herbert Kickl (FPÖ) suspendiert. Begründet wurde das spektakuläre Vorgehen mit dem Verdacht des Amtsmissbrauchs gegen führende Mitarbeiter.

Erhärtet haben sich diese Vorwürfe nicht. Im Parlament gibt es jedoch inzwischen einen Untersuchungsausschuss zur politischen Einflussnahme auf das BVT. Es geht um die Frage, ob die FPÖ nach Übernahme des Innenministeriums auch den Geheimdienst auf Linie bringen wolle. Die Razzia war durch ein anonymes Dossier ausgelöst worden, das der Staatsanwaltschaft von einem hohen Mitarbeiter Kickls übergeben wurde. Auch Belastungszeugen wurden vom Innenministerium präsentiert; eine Zeugin wurde offenkundig zur Aussage gedrängt. Zudem stellte das Ministerium für die Hausdurch-

suchung eine Polizeieinheit ab, die eigentlich für Straßenkriminalität zuständig ist, aber von einem FPÖ-Mann geleitet wird.

Während die Opposition im Untersuchungsausschuss noch über fehlende oder geschwärzte Akten klagte, befeuerten die Veröffentlichungen des Stadtmagazins die Debatten. Das Blatt gibt an, im Besitz einer kompletten Kopie des BVT-Ermittlungsakts zu sein und zitierte aus der Mail eines von den Hausdurchsuchungen betroffenen Mitarbeiters an den Generalsekretär des Justizministeriums. Von einem „Stasi-Krimi" ist da Rede: „Der Angriff erfolgt von innen, teilweise werden hier Institutionen missbraucht, um eine Gewaltenverschiebung in Österreich anzustreben."

Eine BVT-Abteilungsleiterin, aus deren Büro bei der Hausdurchsuchung Material zur rechten Szene in Österreich abtransportiert wurde, klagt in einer Mail an die ermittelnde Staatsanwältin darüber, dass sie bei Ermittlungen gegen Rechtsextremisten „eingeschränkt werde". Sie sieht sich einer „Hetzjagd" ausgesetzt, die sie als „bedrohlich" empfindet. Ein dritter Mitarbeiter schließlich schlägt in einer Mail an seinen Vorgesetzten Alarm, weil bei der Razzia auch eine Festplatte mit hochsensiblen Daten beschlagnahmt worden sei. Zum einen gehe es dabei um eine Liste von Geheimdienst-Quellen, zum anderen um Informationen zur Zusammenarbeit des BVT mit ausländischen Partnerorganisationen wie dem deutschen Bundesnachrichtendienst.

Die BVT-Razzia hinterlässt offenbar schwere Schäden beim Geheimdienst. Intern wuchert das Misstrauen; zudem ist die notwendige Vertrauensbasis zu den Partnerdiensten zerstört. SPÖ-Chef Christian Kern forderte deshalb Kickls Rücktritt. Der Minister selber aber gibt an, man müsse nun in die Zukunft schauen und nicht in die Vergangenheit. Am Tag der Publikation der internen Mails stellte er Reformpläne für den BVT vor. Es werde eine „neue Ära" eingeleitet: „Heute ist der Tag eins eines neuen Staats- und Verfassungsschutzes in Österreich." Sicherer solle das Land werden, transparenter die Behörde. Als Mann, der dies nun schnellstens umsetzen solle, stellte er den alten BVT-Chef Peter Gridling vor. Die von Kickl ausgesprochene Suspendierung hatte das Bundesverwaltungsgericht in der Woche zuvor aufgehoben. Auf die Frage, ob noch eine Vertrauensbasis bestehe, antwortete Kickl: „Sonst würden wir nicht hier sitzen." Gridling versprach, die Aufgabe „professionell wahrzunehmen" (Münch, Mitarbeiter beklagt „Stasi-Krimi", SZ 30./31.05.2018, 8).

Italien

Datenpanne bei Panini

Der italienische Sammelalbenhersteller Panini, der seit über 40 Jahren Alben mit Klebebildchen vertreibt, hatte gravierende Probleme mit der Sicherheit einer Kundendatenbank. Unbefugte hatten persönliche Daten anderer KundInnen einsehen können, darunter viele Bilder von Minderjährigen. Panini bietet über seinen Service „mypanini" den Fans an, Fotos mit dem eigenen Konterfei hochzuladen und sich personalisierte Klebebildchen zuschicken zu lassen. Weltmeisterschaften wie 2018 in Russland sind ein besonders gutes Geschäft: Ein Päckchen mit 5 Bildern kostet 90 Cent, das gesamte WM-Album enthält 682 Motive. Ein Bild können SammlerInnen per Selfie oder Foto individuell gestalten, wobei die Nutzung einer App aus dem Apple oder Google Play Store nötig ist. 10 personalisierte Bildchen kosten 9,90 € und werden per Post zugesendet. Die Februar 2018 gestartete App war ein Erfolg. Auf den Bildern waren häufig Kinder und Kleinkinder zu sehen – viele davon aus Deutschland, aber auch aus Ländern wie Belgien, Frankreich, Brasilien, Argentinien und Australien, manche mit nacktem Oberkörper und im privaten häuslichen Umfeld.

Bis zur Fußballweltmeisterschaft im Juni 2018 haben eingeloggte Anwendende auch die hochgeladenen Bilder sowie personenbezogene Daten anderer KundInnen einsehen können. Auf vielen der Selfie-Sticker waren der volle Name, das Geburtsdatum und auch der Wohnort der Betroffenen verzeichnet. Hackerkenntnisse bedurfte es dafür nicht. Die Bilder konnten über herkömmliche Browser angesteuert werden; ein versehentlicher Vertipper in der URL-Zeile genügte. Auch zahlreiche Bilder von KundInnen, die letztlich gar keine Abzüge bestellten, waren auf diese Weise einsehbar.

Paninis Direktor für Neue Medien, Giorgio Aravecchia, bestätigte am 27.06.2018 das Problem. Es sei intern seit einigen Tagen bekannt und werde schnellstmöglich behoben. Tags darauf erklärte er, die Lücke sei durch ein Sicherheitsupdate geschlossen. Das Unternehmen entschuldigte sich vage für „die Unannehmlichkeiten auf unserer Seite" und versprach, „Ihre Daten künftig besser zu schützen". Wie viele Kundendatensätze betroffen waren, wollte Panini auch nach mehrfacher Nachfrage nicht offenbaren.

Der Hamburger Datenschutzbeauftragte Johannes Caspar bewertete den Vorgang als „besonders problematisch, weil massenhaft Minderjährige betroffen sind". Nach der neu geltenden Datenschutz-Grundverordnung (DSGVO) müsse jedes Unternehmen technisch und organisatorisch für den ausreichenden Schutz personenbezogener Kundendaten sorgen: „Bei einem Verstoß dagegen sowie bei einer Verletzung der Meldepflicht können nun Bußgelder von bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Umsatzes verhängt werden" (Fußball-Sammelbildchen: Datenschutzpanne beim Online-Dienst von Panini, www.heise.de 29.06.2018; Rosenbach, Datenpanne bei Panini, Der Spiegel 27/30.06.2018, 73).

Schweiz

Datenschützer gegen Krankenkassen-Bonus-App

Der Schweizer Datenschutzbeauftragte (EDÖB) Adrian Lobsiger hat beim dortigen Bundesverwaltungsgericht eine Klage gegen die Krankenkasse Helsana eingereicht. Die Datenschützer beanstanden die Verarbeitung der Daten eines Bonusprogramms des Versicherers, der mit Rabatten Versicherte zu mehr Bewegung animieren möchte. Den Datenschützer stört der Datenfluss zwischen gesetzlicher und privater Versicherung. Die Helsana hat die kritisierte Datenverarbeitung vorläufig ausgesetzt, will den Streit aber gegebe-

nenfalls bis vor das höchste Schweizer Gericht bringen.

Die App des Bonusprogramms "Helsana+" soll zu einem bewegungsreicheren Lebensstil und zur Vorsorge animieren und damit die Gesundheit der Teilnehmenden fördern. Sportliche und auch andere gesundheitsfördernde Aktivitäten werden mit Pluspunkten belohnt. Dafür erhalten die Versicherten Barauszahlungen oder geldwerte Rückerstattungen respektive Rabatte bei Partnerfirmen.

Daran hat der Datenschutzbeauftragte grundsätzlich nichts auszusetzen. Allerdings empfahl er der Krankenkasse Ende April 2018, die Übermittlung von Kundendaten zwischen gesetzlicher und privater Krankenversicherung, die von verschiedenen eigenständigen Unternehmensteilen angeboten werden, im Rahmen des Bonusprogramms Helsana+ zu unterlassen. Das Programm steht sowohl Versicherten in der gesetzlichen Grundversorgung als auch KundInnen der privaten Zusatzversicherung der Helsana offen. Für KundInnen der Zusatzversicherung prüft die Kasse intern ab, ob der oder die Versicherte auch Mitglied der Grundversicherung ist. Dafür geben die Versicherten bei der Registrierung für die „Helsana+"-App ihre Einwilligung.

Doch der EDÖB sieht dafür keine Rechtsgrundlage. Eine Entgegennahme dieser Grundversicherungs-Daten durch die Zusatzversicherung und die dort erfolgende Weiterbearbeitung sei in datenschutzrechtlicher Hinsicht generell rechtswidrig und die eingeholten Einwilligungen daher unwirksam. Er verlangte schon im Mai 2018 von der Versicherung, das zu unterlassen.

Darüber hinaus fordert der Datenschutzbeauftragte, die Datenverarbeitung der ausschließlich Grundversicherten im Zusammenhang mit dem Bonusprogramm zu unterlassen. Teilnehmende des Programms können Rückvergütungen ihrer Versicherungsprämien erhalten. Solche Rabatte hält der Datenschützer im Falle von ausschließlich gesetzlich Versicherten für rechtlich unzulässig. Auch für die Querfinanzierung dieser Rabatte aus der privaten Zusatzversicherung gebe es keine rechtliche Grundlage (Sperlich, Schweiz: Datenschützer klagt gegen Krankenkassen-App, www.heise.de 22.06.2018).

Türkei

Flüchtlingsdaten in Deutschland bei AKP

Die türkische Regierungspartei AKP erhielt offenbar von Beschäftigten deutscher Behörden Informationen über Flüchtlinge, die aus der Türkei geflohen waren. Ein Türke erhielt wenige Tage, nachdem er in der Außenstelle des Bundesamts für Migration und Flüchtlinge (BAMF) in Trier seinen Asylantrag gestellt hatte, einen Brief an die ihm vom BAMF zugewiesene Flüchtlingsunterkunft. Darin bat der türkische Präsident und AKP-Chef Recep Tayyip Erdogan darum, ihn und seine Partei bei der Parlaments- und Präsidentschaftswahl am 25.06.2018 zu wählen. Ähnliche aus Deutschland abgeschickte Schreiben haben viele türkische Staatsangehörige in Deutschland erhalten, obwohl in der Türkei Wahlwerbung im Ausland verboten ist. Der betroffene politische Flüchtling ist ein Anhänger der Gülen-Bewegung, die von Erdogan für den gescheiterten Putschversuch Juli 2016 verantwortlich gemacht und deshalb verfolgt wird. Sein Kölner Anwalt Ramazan Sevinc hält es für möglich, dass Beschäftigte vom BAMF oder anderen deutschen Behörden die Adressen an eine türkische diplomatische Vertretung weitergeben: „Anders ist kaum zu erklären, wie die persönlichen Daten meines Mandanten so schnell nach Ankara gelangt sind." Er hält die Sicherheit seines Mandanten für gefährdet. Das BAMF erklärte, dass Schutzsuchende mit vielen Behörden und Dienstleistern zu tun hätten. Im konkreten Fall sein ein Datenschutzdefizit seitens des BAMF nicht feststellbar gewesen (Brisante Wahlwerbung, Der Spiegel Nr. 26 23.06.2018, S. 13).

USA

Kalifornien verabschiedet Internet-Datenschutzgesetz

Gegen den Widerstand vieler Unternehmen im Silicon Valley hat der US-Bundesstaat Kalifornien ein Gesetz für einen besseren Datenschutz von Internetnutzern verabschiedet. Der „California Consumer Privacy Act" wurde am 28.06.2018 vom Senat und Repräsentantenhaus des US-Bundesstaates gebilligt und von Gouverneur Jerry Brown unterzeichnet. Inspiriert von der seit Ende Mai in der EU geltenden Datenschutzgrundverordnung (DSGVO) soll das Gesetz am 01.01 2020 in Kraft treten.

Das Gesetz verpflichtet Unternehmen offenzulegen, welche Kunden- und Nutzerdaten sie speichern. Gleichzeitig sollen kalifornische Nutzende die Möglichkeit erhalten, die Verwendung ihrer persönlichen Daten zu kommerziellen Zwecken zu untersagen. Unter anderem sollen die Internetfirmen einen Link anbieten, mit dem Nutzende ohne großen Aufwand den Weiterverkauf ihrer Daten untersagen können. Gemäß der Einschätzung von Medien und Verbänden ist es das erste Gesetz dieser Art in den USA. Kalifornien reagiert damit auch auf den Skandal beim Internetkonzern Facebook, der wegen seines Umgangs mit persönlichen Daten unter massivem Druck steht.

Dabei ging es um das Abschöpfen von Informationen über 87 Millionen Nutzer, die bei der Datenanalyse-Firma Cambridge Analytica gelandet waren. Die Daten sollen dann unerlaubt für den Wahlkampf des heutigen US-Präsidenten Donald Trump genutzt worden sein; konkrete Beweise für diese These fehlen aber bislang. Google, der Verband der Internet Association, dem auch Amazon und Facebook angehören, sowie Verbände von Handel und Werbewirtschaft hatten sich gegen den Gesetzentwurf ausgesprochen. Auch eine Gesetzesinitiative mit vergleichbaren Zielen, die sich nun erübrigt hat, hatten Google, Amazon, Microsoft, Facebook, mehrere Telefonanbieter und Werbeunternehmen bekämpft (Neues Bundesgesetz verabschiedet Kalifornien nimmt sich EU-Datenschutz zum Vorbild, www.spiegel.de 29.06.2018).

Technik-Nachrichten

Paypal: Fingerabdruck-Authentizierung als Grundeinstellung

Verbraucherschützer kritisieren, dass der Bezahldienst Paypal laut seinen neu veröffentlichten Datenschutzgrundsätzen Fingerabdrücke auf den Smartphones oder Tablets seiner rund 20 Millionen deutschen Nutzenden speichert und nutzt. Damit das Einloggen bei PayPal in der PayPal-App per Fingerabdruck funktioniert, generiert PayPal einen Token und speichert den Token lokal auf dem Gerät. Dieser Token liegt in einer Sandbox-Umgebung, auf die lediglich die PayPal-App zugreifen kann und die lediglich von der PayPal-App gelesen werden kann, wenn der Kunde zum Anmelden seinen Finger auf das Gerät hält. Die PayPal-App oder der PayPal-Server erhalten dabei keinen Zugriff auf die Fingerabdruckdaten.

Carola Elbrecht vom Marktwächter-Team des Bundesverbandes der Verbraucherzentralen (vzbv) erklärte: „Aus meiner Sicht verstößt das gegen den Datenschutz, denn Unternehmen dürfen biometrische Daten wie Fingerabdrücke grundsätzlich nur mit ausdrücklicher Zustimmung ihrer Kunden erfassen." Paypal speichert auch Standortdaten und kann einsehen, welche Apps die Nutzer auf ihren Smartphones oder Tablets installiert haben. Eine Sprecherin des Unternehmens erklärte hierzu, die Nutzenden könnten laut der Datenschutzgrundsätze die Einstellungen ihrer Mobilgeräte ändern, wenn sie die Erfassung der darauf gespeicherten Informationen beschränken wollten. Hierauf erwiderte Verbraucherschützerin Elbrecht, Paypal könnte seine Finanzdienste auch ohne Fingerabdrücke und Standortdaten anbieten.

Der Bezahldienst begründete die Nutzung der Daten damit, so die Sicherheit und die Werbung zu verbessern. So könne Paypal erkennen, wenn Kontozugriffe nicht zum Standort eines Nutzers passen, oder den Nutzern auf Wunsch zum Aufenthaltsort und zu ihren Interessen passende Werbung einspielen. Der US-Bezahldienst hatte seine Datenschutzgrundsätze wegen der seit 25. Mai geltenden neuen EU-Regeln zum Datenschutz überarbeitet (Verbraucherschützer kritisieren Speicherung von Fingerabdrücken bei Paypal, epochtimes.de 31.05./02.06.2018).

Genanlagen haben bedingten Einfluss auf Schulerfolg

Nach einer Analyse des Erbguts von mehr als einer Million Menschen fand eine internationale Forschergruppe 1.271 genetische Varianten, die Einfluss auf den im Leben erreichten Bildungsstand eines Menschen haben sollen. Mit Hilfe von Genanalysen wäre es danach möglich, den Bildungserfolg eines Menschen vorherzusagen.

Wie erfolgreich jemand durch die Schule kommt, hängt jedoch von vielen Einflüssen ab: von den Lehrkräften, der eigenen Motivation, dem Einkommen der Eltern sowie deren Hilfestellung – aber eben auch von den eigenen Genen. Gemäß der Analyse der internationalen Forschergruppe, so deren Veröffentlichung im Fachblatt Nature Genetics, könnten die 1.271 gefundenen Erbanlagen gut zehn Prozent des schulischen Erfolgs erklären. Die genetische Ausstattung ermögliche es, so WirtschaftswissenschaftlerInnen, StatistikerInnen und GenetikerInnen um die Ökonomin Aysu Okbay von der Vrije Universiteit in Amsterdam, sogar zum Teil, den Bildungserfolg eines Menschen vorherzusagen. Okbay befasst sich seit ihrer Doktorarbeit mit der genetischen Basis von wirtschaftlichem und sozialem Erfolg. Zusammen mit mehr als 200 KollegInnen hat sie die genetischen Daten von 1,1 Millionen Menschen ausgewertet. Eine so große Zahl von Versuchsteilnehmenden ist bei solchen sogenannten genetischen Assoziationsstudien notwendig, um halbwegs brauchbare statistische Sicherheit für die zum Teil sehr kleinen Effekte zu bekommen.

Einige der nun identifizierten Genvarianten betreffen die Gehirnentwicklung des Kindes vor und nach der Geburt sowie die Signalübertragung in Nervenzellen. Neben indirekten Einflüssen, zum Beispiel durch das mehr oder weniger fördernde Verhalten der Eltern, entfalte die Genetik sicherlich den stärksten Beitrag über die Beeinflussung der eigenen Gehirnfunktionen, erklärt Markus Nöthen, Direktor des Instituts für Humangenetik an der Uniklinik Bonn: „Natürlich ist die Genetik nicht alleine für den erreichten Bildungsstand verantwortlich, auch dies zeigt sich sehr überzeugend in der vorliegenden Studie. Die Umgebung spielt eine große Rolle. Wahrscheinlich sind genetische und Umgebungseinflüsse aber eng verwoben." Das und die Rolle der Eltern betont auch die Forschergruppe in ihrem Fachaufsatz.

Elsbeth Stern, Professorin für Lehr- und Lernforschung von der Eidgenössischen Technischen Hochschule in Zürich, bezweifelt, dass sich künftig Gentests nutzen lassen, um SchülerInnen gezielt zu fördern. Sobald ein Baby auf der Welt sei, gebe es bessere Indikatoren: „Aus der Art und Weise, wie Babys Objekte anschauen, kann man mehr als 13 Prozent der späteren Intelligenzunterschiede vorhersagen." Auch fast alle Entwicklungsstörungen ließen sich mit größerer Genauigkeit aus Verhaltensbeobachtung ermitteln als mit Genanalysen.

Okbay und ihre KollegInnen weisen selbst darauf hin, dass die Vorhersage des schulischen Erfolgs vor allem für Menschen mit europäischen genetischen Wurzeln funktioniere, bei Versuchsteilnehmenden mit afrikanischer Abstammung die Vorhersagekraft aber deutlich sinke. Sie vermuten, dass dies auch für andere nicht-europäischen Bevölkerungsgruppen der Fall ist; getestet haben sie das aber noch nicht. Laut Elsbeth Stern wäre ein Mangel an Chancengleichheit für Menschen unterschiedlicher Hautfarbe eine Erklärung dafür: „Menschen afroamerikanischer Herkunft erhalten nicht die Entwicklungs- und Lerngelegenheiten, die es ermöglichen, ihr genetisches Potenzial voll auszuschöpfen. Das haben bereits frühere Zwillingsstudien gezeigt" (Charisius, Lesen, Schreiben und Genetik, SZ 24.07.2018, 14).

Rechtsprechung

EGMG

„Recht auf Vergessen" hat Voraussetzungen

Gemäß einem Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 28.06.2018 stand den Mördern des Schauspielers Walter Sedlmayr 2010 kein Recht auf Vergessenwerden zu, da sie einst selbst um eine Berichterstattung in ihrer Sache gebeten haben (Az. 60798/10 und 65599/10). 1990 wurde der bayerische Schauspieler Walter Sedlmayr getötet. Der Fall erregte damals großes öffentliches Interesse in den Medien. Noch heute finden sich im Internet vereinzelt Informationen zu den Umständen der Tat. Die beiden Täter, die, 14 bzw. 15 Jahre nach ihren Verurteilungen wegen Mordes 2007 und 2008 aus der Haft entlassen wurden, wollten von der Öffentlichkeit „vergessen werden". Ein solches Recht gibt es zwar, wurde den Männern jedoch vom Bundesgerichtshof (BGH) mit Urteil vom 09.02.2010 verwehrt (DANA 2/2010, 90). Diese Entscheidung wurde nun vom EGMR bestätigt.

Die beiden Männer hatten gegen drei Medienhäuser (Spiegel, Mannheimer Morgen, Deutschlandfunk) geklagt, die auch noch Jahre nach der Tat über die Ereignisse berichteten und entsprechendes Informationsmaterial in ihren Online-Archiven zur Verfügung stellten. Dort konnten Artikel oder Beiträge eingesehen werden, in denen die Namen der Mörder genannt oder Bilder von ihnen gezeigt wurden. Die Beschwerdeführer sahen dadurch ihr Menschenrecht auf Achtung des Privatlebens (Art. 8 EMRK) verletzt und zogen ohne Erfolg vor den EGMR. Die Straßburger Richter führten aus, dass die Pressefreiheit es Journalisten erlaube, selbst zu entscheiden, welche Details sie veröffentlichen, erst recht dann, wenn wie beim Mord an Sedlmayr ein großes öffentliches Interesse bestehe und die Täter selbst um Berichterstattung in eigener Sache gebeten hätten. 2004 hatten sie die Wiederaufnahme des Verfahrens angestrebt und waren im Zuge dessen selbst an die Medien herangetreten mit der Bitte, erneut über die Einzelheiten zu berichten. Dadurch sei ein Recht auf Vergessenwerden wieder in die Ferne gerückt, so der EGMR.

Dies gelte nur, wenn die Berichterstattung nicht gegen ethische Normen verstoße. Ein solcher Verstoß liege etwa dann vor, wenn die Medien bewusst unwahre Tatsachen verbreiteten. An der Wahrhaftigkeit der Berichterstattung hatte der EGMR jedoch keine Zweifel. Zu berücksichtigen sei auch die nur eingeschränkte Verfügbarkeit der Artikel. Denn um das entsprechende Material abrufen zu können, war es teilweise erforderlich, das jeweilige Medium zu abonnieren bzw. für den Abruf zu zahlen. Eine solche Veröffentlichung in einem Online-Archiv bleibe deutlich zurück hinter einer aktuell abrufbaren Veröffentlichung im Internet oder in einer Mediathek.

Mit seinem Urteil befindet sich der EGMR auf einer Linie mit dem angegriffenen Urteil des BGH. Auch damals wurde dem öffentlichen Interesse an der Berichterstattung der Vorrang gegenüber dem Persönlichkeitsrecht der Täter eingeräumt. Es steht in der Tradition des bekannten Lebach-Urteils des deutschen Bundesverfassungsgerichts aus dem Jahr 1973, bei dem es um die ZDF-Berichterstattung über einen Überfall von zwei Männern auf ein Munitionsdepot nahe der saarländischen Kleinstadt Lebach ging, bei der vier Soldaten ermordet worden waren und bei dem Homosexualität eine Rolle gespielt hatte. Auch der EGMR bekräftigte die Bedeutung des „Rechts auf Vergessen", gerade in Zeiten des Internets, weshalb die Frage der Datenlöschung immer auch unter dem Aspekt der inzwischen verflossenen Zeit zu beantworten ist. Der EGMR stellte bei seinem Urteil auf das Jahr 2010 ab. Dies kann zur Folge haben, dass bei dem Fall im Jahr 2018, also eine Dekade nach der Entlassung und mehr als ein Vierteljahrhundert nach dem Mord, der Resozialisierung der Vorrang einzuräumen ist. Die Spiegel-Verlagsgruppe, deren Online-Portal „Spiegel Online" ein Dossier über die Geschichte des Mordes zum Abruf bereitgestellt hatte, begrüßte die Entscheidung: „Die im öffentlichen Interesse liegende Funktion eines Online-Archivs als ‚historisches Gedächtnis' einer Gesellschaft bleibt damit erhalten" (Kein Recht auf Vergessenwerden für Sedlmayr-Mörder, www.lto.de 28.06.2018; Janisch, Ewig am Pranger, SZ 29.06.2018, 1).

EuGH

Datensammeln der Zeugen Jehovas unterfällt Datenschutz

Mit Urteil vom 10.07.2017 entschied der Europäische Gerichtshofs (EuGH) in Luxemburg, dass die personenbezogenen Daten, die anlässlich der Hausbesuche der Glaubensgemeinschaft der Zeugen Jehovas anfallen, unter das europäische Datenschutzrecht fallen (C-25/17). Im Rahmen ihrer sogenannten Verkündigungstätigkeit gehen die Mitglieder der Zeugen Jehovas von Haus zu Haus und klingeln, um mit den BewohnerInnen zu sprechen. 2013 hatte die Tietosuojalautakunta, die finnische Datenschutzkommission, den Zeugen Jehovas verboten, sich Notizen zu machen, ohne auf den Datenschutz zu achten. Die finnischen Mitglieder der Religionsgemeinschaft schrieben offenbar nicht nur die Adressen der Befragten auf, sondern hielten auch fest, welche religiösen Überzeugungen die Befragten haben und in welchen Familienverhältnissen sie leben. Diese Informationen fließen laut Darstellung des Gerichts in Gebietskarten ein, mit denen die Rundgänge organisiert werden.

Die Daten werden gemäß dem EuGH als Gedächtnisstütze erhoben, um für den Fall eines erneuten Besuchs wiederauffindbar zu sein, ohne dass die betroffenen Personen hierin eingewilligt hätten oder darüber informiert worden wären. Außerdem führen die Gemeinden der Gemeinschaft eine Liste der Personen, die darum gebeten haben, nicht mehr von den Verkündigern aufgesucht zu werden. Die in dieser Liste enthalte-

nen personenbezogenen Daten werden von den Mitgliedern der Gemeinschaft verwendet.

Ähnlich wie die finnische Datenschutzbehörde sieht auch der EuGH in der Tätigkeit der Zeugen Jehovas – anders als von diesen vorgebracht – keine ausschließlich persönliche oder familiäre Tätigkeit, wofür die Datenschutzregeln nicht gelten würden. Der Umstand, dass die Verkündungstätigkeit von Tür zu Tür durch das in Art. 10 Abs. 1 Grundrechte-Charta verankerte Grundrecht auf Gewissens- und Religionsfreiheit geschützt ist, verleihe ihr keinen ausschließlich persönlich-familiären Charakter, da sie über die private Sphäre eines als VerkünderInnen tätigen Mitglieds der Religionsgemeinschaft hinausgeht. Dass die Daten nicht digital, sondern handschriftlich vorliegen, ändere nichts daran, dass Daten gesammelt würden. Diese seien zudem durchaus nach bestimmten Kriterien als „Datei" strukturiert, damit man sie später leichter finden könne.

Das Gericht entschied, dass „eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitung personenbezogener Daten angesehen werden kann." Diese Akteure können in verschiedenen Phasen und in unterschiedlichem Ausmaß in die Verarbeitung einbezogen sein, so dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist. Der Gerichtshof stellte außerdem fest, dass aus keiner Bestimmung des Unionsrechts geschlossen werden kann, dass die Entscheidung über die Zwecke und Mittel der Verarbeitung mittels schriftlicher Anleitungen oder Anweisungen seitens des für die Verarbeitung Verantwortlichen erfolgen muss. Hingegen kann eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung der personenbezogenen Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung beteiligt ist, als für die Verarbeitung Verantwortlicher angesehen werden. Im Übrigen setze die gemeinsame Verantwortlichkeit mehrerer Akteure nicht voraus, dass jeder von ihnen Zugang zu den personenbezogenen Daten hat.

Der Fall kam vor den EuGH, weil der Korkein hallinto-oikeus, der Oberste Verwaltungsgerichtshof Finnlands, an den EuGH ein sogenanntes Vorabentscheidungsersuchen gerichtet hatte. Über diesen Weg können Gerichte der EU-Mitgliedstaaten in einem bei ihnen anhängigen Rechtsstreit auf EU-Ebene erfragen, wie der EuGH die Rechtsfragen sieht. Ein nationales Urteil ersetzt der EuGH-Spruch aber nicht (Tack, EuGH-Urteil Zeugen Jehovas müssen bei Hausbesuchen auf Datenschutz achten, www.spiegel.de 10.07.2018; EuGH, PM Nr. 103/18 v. 10.07.2018).

BVerwG

De-CIX-Klage gegen strategische TK-Überwachung des BND abgewiesen

Gemäß einem Urteil des Bundesverwaltungsgerichts (BVerwG) in Leipzig vom 30.05.2018 in erster und letzter Instanz darf der Bundesnachrichtendienst (BND) weiterhin am Internet-Knoten De-CIX aus Frankfurt am Main anlasslos Daten abgreifen (Az. 6 A 3.16). Dies wollte der Betreiber von De-CIX mit seiner Klage unterbinden. Das BVerwG stellte fest, der Betreiber könne verpflichtet werden, bei der strategischen Fernmeldeüberwachung durch den BND mitzuwirken. Der Geheimdienst sei berechtigt, auf Anordnung des Bundesinnenministeriums internationale Telekommunikation zu überwachen und aufzuzeichnen.

Der BND zapft nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz) seit Jahren zu Aufklärungszwecken in großem Stil Daten aus dem – nach Verkehrsaufkommen – größten Internet-Knotenpunkt der Welt ab. Dabei erhalten die Geheimdienstler die Daten nicht nur aufgrund eines konkreten Tatverdachts, sondern im Zuge der strategischen Fernmeldeüberwachung, also anlasslos. Rechtsanwalt Sven-Erik Heun erklärte für die Klägerseite in der rund dreistündigen Verhandlung: „Der BND hat sich den größten Teich ausgesucht, in dem er fischen kann." Wer sich an De-CIX wende, bekomme einen riesigen Datensatz, in dem auch nationaler Telekommunikationsverkehr vorhanden ist, was nach Ansicht von Heun rechtswidrig ist. Außerdem erhebe der BND den Datenverkehr eines bestimmten Protokolls vollständig, ohne die gesetzlich vorgesehene quantitative Beschränkung auf 20 Prozent.

Aus Sicht des De-CIX ließen die Anordnungen aus dem Bundesinnenministerium überdies nicht erkennen, ob sie das zuständige Kontrollgremium des Bundestags durchlaufen haben. Im Zuge des NSA-Untersuchungsausschusses war herausgekommen, dass bei De-CIX abgegriffene Daten über den BND wahrscheinlich an die NSA gelangten. Dagegen machte Rechtsanwalt Wolfgang Roth für die Bundesregierung geltend, als Schutz für von Überwachungen Betroffene gebe es die G-10-Kommission des Bundestages, welche die Eingriffe in das Fernmeldegeheimnis erlaube. Eine detailliertere Anordnung könne es aufgrund der Geheimhaltung aber nicht geben, erklärte Roth.

Dieser Argumentation folgte der 6. Senat des BVerwG. Dem gemäß legt das Bundesinnenministerium die Übertragungswege sowie den Umfang des Überwachungsmaterials fest und kann einen Betreiber von Telekommunikationsdiensten, wie De-CIX, verpflichten, den BND bei der Überwachung zu unterstützen. Ob und in welchem Umfang das verpflichtete Unternehmen Vorkehrungen zu treffen hat, richte sich letztlich nach § 27 Abs. 2 der Telekommunikations-Überwachungsverordnung (TKÜV). Danach hat der Verpflichtete dem BND an einem Übergabepunkt im Inland eine vollständige Kopie der Telekommunikation bereitzustellen, die über die in der Anordnung bezeichneten Übertragungswege übertragen wird. Auf der Grundlage der Beschränkungsanordnung wählt der BND gegenüber dem Telekommunikationsdiensteanbieter diejenigen Übertragungswege aus, die überwacht werden sollen. Die Haftung und Verantwortung liege nicht beim Betreiber, sondern beim Bundesinnenministerium. Die Betreiber von De-CIX könnten sich als reine TK-Vermittler auch nicht auf den Schutz des Fernmeldegeheimnisses des Art. 10 Grundgesetz (GG) berufen.

Die Betreiber des Internetknotens De-CIX wollen gegen das Urteil mit einer

Beschwerde beim Bundesverfassungsgericht vorgehen, um sich nicht länger als Komplizen bei den damit verknüpften Eingriffen ins Fernmeldegeheimnis verdingen zu lassen, so Klaus Landefeld, Aufsichtsrat der Management-Gesellschaft: „Wir sind uns mit unserem Gang nach Karlsruhe sehr sicher". Die ausgemachten „umfassenden Verstöße" gegen Art. 10 GG und das darin verbriefte Kommunikationsgeheimnis hatte De-CIX zwar in das Verfahren in Leipzig eingebracht und detailliert dargelegt. Sie seien jedoch vom BVerwG „aus für uns nicht nachvollziehbaren Gründen" nicht behandelt worden. Die Leipziger Entscheidung werfe Fragen zum effektiven Rechtsschutz auf. So könnten BürgerInnen ohne die erforderlichen Detailkenntnisse nicht darlegen, dass sie selbst von der BND-Überwachung in Frankfurt betroffen seien. Die verpflichteten Unternehmen wiederum dürften die Rechte der BürgerInnen nicht geltend machen.

Parallel plant die De-CIX-Managementgesellschaft laut Landefeld eine zweite Klage vor dem BVerwG. Auf diesem Weg solle sichergestellt werden, dass „die eigenen Grundrechte des Unternehmens und seiner Mitarbeiter als Kommunikationsteilnehmer geltend gemacht und effektiv sichergestellt werden können" (Gerichtsurteil: BND darf weiterhin Internet-Knoten De-CIX anzapfen, www.heise.de 31.05.2018; BVerwG, PM Nr. 38/2918 v. 31.05.2018, Klage der DE-CIX Management GmbH erfolglos; Krempl, BND-Überwachung: De-CIX-Betreiber will vors Bundesverfassungsgericht, www.heise.de 31.05.2018).

VGH Baden-Württemberg

Schleierfahndungsregelung zu unbestimmt

Der Verwaltungsgerichtshof (VGH) Baden-Württemberg in Mannheim bestätigte mit Urteil vom 13.02.2018 eine Entscheidung des Verwaltungsgerichts (VG) Stuttgart, dass die Ermächtigung zur sog. Schleierfahndung in § 23 Abs. 1 Bundespolizeigesetz (BPolG) europarechtswidrig sei (1 S 1469/17). Ein aus Afghanistan stammender Deutscher war im ICE von Berlin nach Freiburg in der Gegend von Offenburg als einziger von mehreren Personen im Erste-Klasse-Bereich kontrolliert worden. Die Vorschrift verstoße wegen Unbestimmtheit gegen den Schengener Grenzkodex. Die mit „VS-nfD" (Verschlusssache – nur für den Dienstgebrauch) überschriebenen internen Weisungen der Bundespolizei seien keine wirksamen Begrenzungen behördlichen Handelns. Der VGH weist im Rahmen der Entscheidung darauf hin, dass aufgrund der Rechtsprechung des Europäischen Gerichtshofs (EuGH) – abweichend von früherer Rechtsprechung des Bundesverwaltungsgerichts – Verwaltungsvorschriften öffentlich bekannt zu machen sind. Das VG Stuttgart hatte die Berufung ausdrücklich zugelassen, weil durch die millionenfachen Kontrollen durch die Bundespolizei das Verfahren Grundsatzbedeutung habe. Der VGH ließ allerdings die Revision nicht zu (ANA-ZAR 2/2018, 21).

BGH

Erben haben Zugriff auf Verstorbenen-Accounts

Der Bundesgerichtshof (BGH) in Karlsruhe hat mit einem Urteil vom 12.07.2018 letztinstanzlich entschieden, dass Erben auf das Facebook-Konto eines Verstorbenen zugreifen dürfen (Az. III ZR 183/17). Die Richter hoben damit ein Urteil des Berliner Kammergerichts (KG) auf, das die bisherige Sperre unter Verweis auf das Fernmeldegeheimnis bestätigt hatte (DANA 3/2017, 176 f., zur Vorentscheidung des LG Berlin DANA 1/2016, 40 f.).

Der Vorsitzende Richter Ulrich Herrmann begründete die Entscheidung bei der Urteilsverkündung damit, dass auch Briefe und Tagebücher an die Erben übergehen. Es bestehe kein Grund, digitale Inhalte anders zu behandeln. Die Tochter habe mit Facebook einen Nutzungsvertrag geschlossen, und die Eltern seien als Erben in diesen Vertrag eingetreten. Durch Facebooks Bestimmungen sei ein Vererben des Vertrags nicht ausgeschlossen. Konkret ging es um den Zugang zum Facebook-Account eines 15-jährigen Mädchens, das in Berlin 2012 unter ungeklärten Umständen von einer U-Bahn erfasst worden war und später im Krankenhaus starb.

Die Eltern wünschen sich Gewissheit darüber, ob es sich um einen Unfall oder einen Suizid gehandelt hat. Daher wollten sie wissen, welche Nachrichten ihre Tochter auf Facebook ausgetauscht hat. Als Klägerin trat die Mutter auf. Sie hofft zudem, dass ihr die Nachrichten helfen, Schadenersatzansprüche des U-Bahn-Fahrers abzuwehren.

Nach eigener Aussage kannten die Eltern das Facebook-Passwort des Mädchens, das sich mit 14 Jahren im Netzwerk angemeldet hatte. Als sie sich aber nach dessen Tod in sein Konto einloggen wollten, klappte das nicht mehr: Das Konto befand sich bereits im sogenannten Gedenkzustand, einem Profilstatus für Verstorbene. Facebook hatte das nach dem Hinweis eines den Eltern unbekannten Nutzers auf den Tod des Mädchens veranlasst. Wird ein Konto in den „Gedenkzustand" versetzt, bleibt das Profil als eine Art virtuelles Kondolenzbuch online und ist für alle Nutzenden sichtbar, die es auch vorher sehen konnten.

Facebook weigerte sich auf Nachfrage, den Eltern Zugriff auf das Konto und die Chatnachrichten des Mädchens zu geben; die Mutter zog deshalb gegen das Unternehmen vor Gericht. Facebook rechtfertigte seine Haltung damit, dass der „Gedenkzustand" nicht nur die Rechte toter Nutzender schütze, sondern auch die von ihren Facebook-Kontakten. Diese würden davon ausgehen, dass private Nachrichten privat bleiben.

Der Vorsitzende Richter Ulrich Herrmann hatte die Position von Facebook in der Verhandlung bereits kritisch hinterfragt: Mit dem Passwort hätten sich die Eltern schon zu Lebzeiten des Mädchens im Konto anmelden können. Es sei damit fraglich, ob das Vertrauen der anderen Nutzenden, dass niemand mitlese, wirklich schutzwürdig sei.

Vor der Entscheidung war umstritten, ob digitale Inhalte vererbt werden können, insbesondere Daten, die sich nicht – vergleichbar mit dem Tagebuch – ausschließlich zu Hause auf der Festplatte oder einem Datenträger befinden, sondern auf einem fremden Server. Die Richter haben nun entschieden, dass der Vertrag über ein Benutzerkonto bei einem sozialen Netzwerk grundsätzlich

im Rahmen der Gesamtrechtsnachfolge nach § 1922 Abs. 1 BGB auf die Erben des ursprünglichen Kontoberechtigten übergeht. Dessen Vererblichkeit sei nicht durch die vertraglichen Bestimmungen ausgeschlossen. Die Nutzungsbedingungen enthalten hierzu keine Regelung. Die Klauseln zum Gedenkzustand sind bereits nicht wirksam in den Vertrag einbezogen. Sie hielten überdies einer Inhaltskontrolle nach § 307 Abs. 1 und 2 BGB nicht stand und wären daher unwirksam. Diese hätten gegenüber dem Netzwerkbetreiber so einen Anspruch auf Zugang zu dem Konto einschließlich der darin vorgehaltenen Kommunikationsinhalte.

Aus dem Wesen des Vertrags ergebe sich nicht eine Unvererblichkeit des Vertragsverhältnisses; dieser sei nicht höchstpersönlicher Natur. Der höchstpersönliche Charakter folge nicht aus im Nutzungsvertrag stillschweigend vorausgesetzten und damit immanenten Gründen des Schutzes der Persönlichkeitsrechte der Kommunikationspartner der Erblasserin. Zwar mag der Abschluss eines Nutzungsvertrags mit dem Betreiber eines sozialen Netzwerks in der Erwartung erfolgen, dass die Nachrichten zwischen den Teilnehmenden des Netzwerks jedenfalls grundsätzlich vertraulich bleiben und nicht durch die Beklagte dritten Personen gegenüber offengelegt werden. Die vertragliche Verpflichtung Facebooks zur Übermittlung und Bereitstellung von Nachrichten und sonstigen Inhalten sei jedoch von vornherein kontobezogen. Sie habe nicht zum Inhalt, diese an eine bestimmte Person zu übermitteln, sondern an das angegebene Benutzerkonto. Der Absender einer Nachricht könne dementsprechend zwar darauf vertrauen, dass die Beklagte sie nur für das von ihm ausgewählte Benutzerkonto zur Verfügung stellt. Es besteht aber kein schutzwürdiges Vertrauen darauf, dass nur der Kontoinhaber und nicht Dritte von dem Kontoinhalt Kenntnis erlangen. Zu Lebzeiten müsse mit einem Missbrauch des Zugangs durch Dritte oder mit der Zugangsgewährung seitens des Kontoberechtigten gerechnet werden und bei dessen Tod mit der Vererbung des Vertragsverhältnisses.

Eine Differenzierung des Kontozugangs nach vermögenswerten und höchstpersönlichen Inhalten scheide aus. Nach der gesetzgeberischen Wertung gingen auch Rechtspositionen mit höchstpersönlichen Inhalten auf die Erben über. Analoge Dokumente wie Tagebücher und persönliche Briefe würden auch vererbt, wie aus § 2047 Abs. 2 und § 2373 Satz 2 BGB zu schließen ist. Es bestehe aus erbrechtlicher Sicht kein Grund dafür, digitale Inhalte anders zu behandeln. Einen Ausschluss der Vererblichkeit auf Grund des postmortalen Persönlichkeitsrechts der Erblasserin verneinte der III. Zivilsenat ebenfalls. Auch das für das KG in seinem Urteil entscheidende Fernmeldegeheimnis (Art. 10 GG) stehe dem Anspruch der Klägerin nicht entgegen, da der Erbe, der vollständig in die Position des Erblassers einrückt, jedenfalls nicht „anderer" im Sinne von § 88 Abs. 3 TKG sei.

Bei einer Datenschutzprüfung, für die der BGH die neue DSGVO anwenden musste, ergab sich kein anderes Ergebnis. Die der Übermittlung und Bereitstellung von Nachrichten und sonstigen Inhalten immanente Verarbeitung der personenbezogenen Daten der Kommunikationspartner der Erblasserin sei nach Art. 6 Abs. 1 lit. b Var. 1 und lit. f DSGVO zulässig, also zur Erfüllung der vertraglichen Verpflichtungen gegenüber den Kommunikationspartnern der Erblasserin als auch auf Grund berechtigter überwiegender Interessen der Erben.

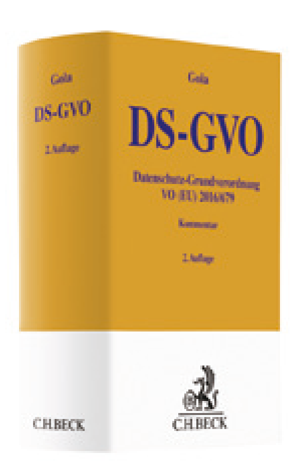
Die Mutter erklärte: „Wir sind überaus erleichtert über die Entscheidung des BGH. Facebook hat immer betont, anhand unseres Falles Rechtssicherheit gewinnen zu wollen. Sie ist nun hergestellt und darum hoffen wir sehr, dass das Unternehmen uns nun umgehend Zugang zu dem Account unserer Tochter gewährt und uns nicht weitere Wochen, Monate oder gar Jahre des quälenden Wartens zumutet." Ein Facebook-Sprecher erklärte derweil, das Abwägen zwischen den Wünschen von Angehörigen und dem Schutz der Privatsphäre Dritter sei eine der schwierigsten Fragen, die sich das Unternehmen stelle müsse: „Wir fühlen mit der Familie. Gleichzeitig müssen wir sicherstellen, dass der persönliche Austausch zwischen Menschen auf Facebook geschützt ist. Wir haben inhaltlich eine andere Position vertreten und der langwierige Prozess zeigt, wie komplex der verhandelte Sachverhalt ist" (BGH-Urteil Facebook muss Eltern Zugriff auf Nachrichten verstorbener Tochter gewähren, www.spiegel.de 12.07.2018; BGH, PM Nr. 115/2018 v. 12.07.2018, Vertrag über ein Benutzerkonto bei einem sozialen Netzwerk ist vererbbar).

Cartoon



Bild: Frans Valenta

Buchbesprechungen



Gola, Peter (Hrsg.)
DS-GVO – Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar
C.H.Beck 2. Aufl. 2018, 1092 S., ISBN 978-3-406-72007-9, 85,- €

(wh) Die hier vorliegende Auflage ist bereits ca. ein Jahr nach der ersten Auflage, die in der DANA 2/2017 (S. 115) besprochen wurde, erschienen. Laut Vorwort zur zweiten Auflage wird die „kurzfristig erschienene zweite Auflage“ vom Verlag damit begründe, dass inzwischen „der nationale Gesetzgeber – innerhalb des von ihm möglicherweise zu großzügig eingeschätzten Erlaubnisrahmens – Regelungen zur Ergänzung der Datenschutz-Grundverordnung in einer Neufassung des Bundesdatenschutzgesetzes und weiteren Bereichsspezifischen Gesetzen geschaffen hat“. Des Weiteren wurden zwischenzeitlich erschienene Kommentierungen der DS-GVO und des neuen BDSG berücksichtigt. Dies erklärt auch den deutlichen Seitenzuwachs gegenüber der ersten Auflage.

Die grundsätzlichen Aussagen der Besprechung der ersten Auflage („Die Qualität der Kommentierung ist durchgängig erfreulich.“ „insbesondere für die PraktikerIn erkenntnisfördern“, „für die wissenschaftliche Tiefe ist dann aber doch noch ein Rückgriff auf weitere Literatur nötig, wobei auf diese sehr zahlreich verwiesen wird.“) gelten auch für die zweite Auflage. Dies gilt leider auch für die in der Rezension der ersten Auflage genannten inhaltlichen Kritikpunkte (z.B. Konflikt zwischen Berufsgeheimnissen und Datenschutzkontrolle mit Vorrang für das Berufsgeheimnis, werbefreundliche Auslegung des Art. 22, nahezu unkritisches Referieren der Beschränkungen der §§ 32 bis 36 BDSG). Der Kommentar lässt leider offen, an welchen Stellen der nationale Gesetzgeber die sogenannten Öffnungsklauseln der DSGVO „möglicherweise zu großzügig“ genutzt hat. Auch der vom deutschen Bundesinnenministerium geprägte Begriff der „Öffnungsklauseln“, bei denen es sich nach der EU-Kommission nur um Konkretisierungs- und Regelungsklauseln handelt, wird unkritisch übernommen.

Die Verknüpfung der Kommentierung der Artikel der DSGVO mit der direkt anschließenden Kommentierung der gegebenenfalls ergänzenden Paragraphen des BDSG kann nur als gelungen bezeichnet werden, da diese Gestaltung der Kommentierung die Arbeit mit der DSGVO und dem BDSG wesentlich erleichtert.

Alles in allem ist auch die zweite Auflage – die vermutlich wegen des gestiegenen Umfangs im Preis um sechs Euro gestiegen ist – eine lohnenswerte Anschaffung für PraktikerInnen im Datenschutz.



Paal, Boris P./Pauly, Daniel (Hrsg.)
Datenschutz-Grundverordnung – Bundesdatenschutzgesetz,
C.H.BECK-Verlag, 2. Aufl. 2018, 1260 S., ISBN 978-3-406-71838-0, 129,- €

(wh) Auch dieser Kommentar liegt nun in der zweiten Auflage vor. Während die erste Auflage, die in der DANA 1/2017 (S. 67) besprochen wurde, sich noch ganz auf die EU-Datenschutz-Grundverordnung (DSGVO) beschränkte bezieht die zweite Auflage nun das am 25. Mai 2018 in Kraft getretene BDSG mit ein. Dies führt zu einer deutlichen Umfang- und Preissteigerung. Auch das AutorInnen-Team wurde gegenüber der Erstauflage um drei BearbeiterInnen erweitert. Die Zunahme des Umfangs ist – laut dem Vorwort zur 2. Auflage „in erster Linie der Verdopplung der Rechtsquellen geschuldet.“

Bei diesem Kommentar ist es – im Gegensatz zum im gleichen Verlag erschienenen Werk Gola, Peter (Hrsg.) „DS-GVO – Datenschutz-Grundverordnung“ (s.o.), dass die Paragraphen des neuen BDSG nicht direkt hinter den entsprechenden Artikeln kommentiert werden, sondern erst die DSGVO und dann das BDSG kommentiert wird. Dies führt zu einem höheren Aufwand beim Blättern, was aber dem Inhalt der Kommentierungen keinen Abbruch tut.

Auch wenn sich die Inhaltsverzeichnisse der einzelnen Kommentierungen in der 2. Auflage gegenüber der Erstauflage geändert haben, ist doch der Bezug zu den entsprechenden Abschnitten über die Randnummern möglich. Dies führt allerdings dazu, dass es Randnummern wie 1a, 1b, etc. gibt.

Bei der Kommentierung des BDSG ist es den AutorInnen – wie bereits bei der Kommentierung der DSGVO – gelungen, die Rechtsmaterie so darzustellen, dass sie für die LeserInnen handhabbar ist, da hier die Regelungen des neuen BDSG mit den entsprechen Artikeln der DS-GVO und deren Kommentierung in Bezug gesetzt werden. Wie schon für die Erstauflage vermerkt, kommen auch in der Zweitauflage praktische Anwendungsfragen zwangsläufig oft zu kurz.

Allerdings sind die DatenschutzpraktikerInnen auch nicht explizit in der Zielgruppe aufgeführt, sondern „Rechtsanwaltschaft, Justiz, Unternehmen, Behörden, Verbände und Wissenschaft". Die Aussage aus der Rezension der Erstauflage „Insofern ist die Kommentierung eine nützliche Hilfe" gilt aber uneingeschränkt auch für die zweite Auflage.



Däubler, Wolfgang; Wedde, Peter; Weichert, Thilo; Sommer, Imke
EU-Datenschutz-Grundverordnung und BDSG-neu – Kompaktkommentar
BUND Verlag, 2018, 1379 S., ISBN 978-3-7663-6615-3, 99,- €

(wh) Die Schwerpunkte dieses sehr umfangreichen Kompaktkommentars liegen insbesondere auf dem Beschäftigtendatenschutz, den Auswirkungen des neuen Datenschutzrechts auf Interessenvertretungen der Beschäftigten und der Umsetzung der Betroffenenrechte. Neben der DSGVO und dem am 25. Mai 2018 in Kraft getretenen Bundesdatenschutzgesetz (BDSG) sind – auch wenn der Titel des Kommentars dies verschweigt – weitere bereichsspezifische Regelungen, die insbesondere – aber nicht nur – im Beschäftigtendatenschutz relevant sind, aufgeführt worden. Hierzu gehören Auszüge aus dem Telemediengesetz (TMG), das Unterlassungsklagegesetz (UKlaG) und das Sicherheitsüberprüfungsgesetz (SÜG) sowie im Anhang unkommentiert einzelne Paragraphen aus dem UWG (§ 7, der als Umsetzung von Art. 13 der ePrivacy-Richtlinie, hier im Kommentar TK-DS-Richtlinie genannt, weiterhin gültig ist), dem StGB (§ 203) und dem KunstUrhG (§ 23).

Etwas unpraktisch ist auch hier, dass die die DSGVO ergänzenden Paragraphen des neuen BDSG nicht direkt hinter den entsprechenden Artikeln kommentiert werden, sondern erst die DSGVO und dann das BDSG kommentiert wird. Dies führt zu einem höheren Aufwand beim Blättern, was aber dem Inhalt der Kommentierungen keinen Abbruch tut.

Beim der Kommentierung des TMG ist etwas irritierend, dass die ePrivacy-Verordnung (ePrivVO) in der Fassung des Entwurfs der EU-Kommission abgedruckt wird. Da es bereits im Oktober 2017 eine Entscheidung des EU-Parlaments mit einer abgeänderten Fassung des Kommissionsentwurfs gibt und derzeit noch gar nicht absehbar ist, wie die ePrivVO nach den Trilog-Verhandlungen aussehen wird, wäre dieser Abdruck an dieser Stelle entbehrlich gewesen. Erfreulich ist bei der Kommentierung des TMG aber, dass jeweils angegeben wird, ob die jeweilige Regelung auf der durch die DSGVO abgelöste EU-Datenschutzrichtlinie und/oder auf der durch die DSGVO nicht berührte ePrivacy-Richtlinie basiert. Dies erleichtert die Einschätzung, ob eine Regelung des TMG durch die DSGVO verdrängt wird oder nicht.

Beim UKlaG und dem SÜG gibt es jeweils eine umfassende Einführung. Kommentiert werden aber nur die für die Thematik Datenschutz relevanten Paragraphen, was der Übersichtlichkeit dient.

Nicht nur durch den Verlag, sondern auch durch den Inhalt wird deutlich, dass die Zielgruppe dieses Kommentars betriebliche und behördliche Datenschutzbeauftragte, Betriebs- und Personalräte sowie Personalabteilungen sind. Aber auch allen, die aus anderen Gründen am Beschäftigtendatenschutz interessiert sind, ist dieser Kommentar sehr zu empfehlen.



Schulte, Laura
Vom quantitativen zum qualitativen Datenschutz
Leitbildwandel im Datenschutzrecht
Duncker&Humblot Berlin 2018, ISBN 978-3-428-15389-3, 308 S., 89,90 €

(tw) Angesichts der Masse existierender Datenschutzliteratur ist es verwunderlich, dass sich bisher nur wenige AutorInnen daran gemacht haben, die Geschichte des nationalen deutschen Datenschutzgesetzgebers umfassend nachzuvollziehen und einer qualitativen Bewertung zu unterwerfen. Die Einleitung des früheren Simitis-Kommentars zum BDSG enthielt eine stark normativ-deskriptiv gehaltene Darstellung. Es blieb ein Defizit hinsichtlich einer übergeordneten Einordnung. Dieses Defizit ist mit der Dissertation von Laura Schulte behoben. Mit dem nicht ganz eingängigen Titel legt die Autorin eine umfassende Studie über die allgemeine Datenschutzgesetzgebung von ihren ersten Anfängen in den 70er Jahren bis zum heutigen Zeitpunkt in Form des DSGVO-Anpassungs- und -Umsetzungsgesetzes vor. Dabei irritiert der nicht überzeugende Begriff des „quantitativen Datenschutzes", mit dem ein eindimensionaler, an Ge- und Verboten orientierter Rechtsrahmen beschrieben wird, dem eine „qualitativer Datenschutz" entgegengestellt wird, der die unterschiedlichsten normativen, prozeduralen und technisch-organisatorischen Regelungselemente beinhaltet und nicht nur auf Ordnungsrecht, sondern auch auf die Gestaltung des Marktgeschehens setzt.

Schulte erzählt unter ausführlicher Darstellung der Diskussionsgrundlagen und -beiträge die Entwicklung vom ersten Datenschutzgesetz bis zur Umsetzung europäischer Vorgaben und kommt zu dem Schluss, dass der Gesetzgeber der technischen Entwicklung regelmäßig hinterherhinkte und zumindest in der neueren Zeit nur noch reagierte, nicht aktiv gestaltete. Dabei fragt sie, von welchen Leitbildern dieser bestimmt war, also von welchen faktischen, theoretischen

und normativen Grundannahmen, die sie mit unterschiedlichen Begriffen kennzeichnet: Privatheit, Rationalisierung, Markt, Sicherheit, Systemschutz und, wie es Schulte nennt, e-Privacy, also das Zusammenspiel von Recht und Technik zur Ermöglichung grundrechtskonformer Online-Kommunikation. Dabei geht sie auf die wichtigen markanten Wegweisungen ein, etwa die ersten Arbeiten auf Landesebene, die Sicherheitsdebatten der 70er Jahre, das Volkszählungsurteil, die europäische Richtlinie, die Entwicklung der Bereichsspezifik, die Rezeptionen aus dem Medien- und dem IT-Sicherheitsrecht, die Debatten um den Datenschutz in der (Online-) Wirtschaft, das Grundrechte auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und schließlich die DSGVO, aber auch detailverliebt auf einzelne Ereignisse, Vorschläge und Meinungsäußerungen.

Anders als viele Dissertationen tastet sich die Arbeit nicht erst an das Thema heran, um es am Ende einigermaßen erfasst zu haben, sondern beschränkt sich von Anfang an auf das Wesentliche in kompetenter und verständlicher Weise, was von einer umfassenden Durchdringung der Materie zeugt, um dann in grundrechtsfreundlicher Weise und mit klaren Worten die jeweiligen Gesetzgebungsaktivitäten normativ und technisch, sowie mit Eingeschränkungen im politischen und ökonomischen Kontext einzuordnen. Erfrischend ist dabei die Leichtigkeit, mit der die Autorin zwischen jeweiligen Einzelnormen und dahinter stehenden Grundsatzüberlegungen hin- und herspringt. Dabei greift sie durchgehend auf die Originalunterlagen zurück, so dass die Arbeit auch als Quellenfundbuch verwendet werden kann, unterlässt es aber nicht, einen ausgewogenen Blick in die üppige Literatur zu nehmen. Ein umfangreiches Inhalts-, Literatur- und Sachverzeichnis ermöglicht die zeitübergreifende Erfassung sowie die Vertiefung von Einzelaspekten. Also: Wem es nicht nur um Anwendung, sondern um ein Grundverständnis von Datenschutzentwicklungen geht, dem sei dieses Buch wärmstens empfohlen.



Müller-Heidelberg, Till/Pelzer, Marei/Heiming, Martin/Röhner, Cara/Gössner, Rolf/Fahrner, Matthias/Pollähne, Helmut/Seitz, Maria (Hrsg.)
Grundrechte-Report 2018 – Zur Lage der Bürger- und Menschenrechte in Deutschland
Fischer Taschenbuch, Frankfurt/Main 2018, 240 S., 10,99 €, ISBN 978-3-596-70189-6

(tw) Volker Beck präsentierte am 29.05.2018 in Karlsruhe den Grundrechte-Report 2018, den alternativen – oder nach anderer Lesart den wahren – Verfassungsschutzbericht mehrerer Bürgerrechtsorganisationen. Der Bericht ist wieder ein Spiegel der aktuell geführten Grundrechtsdiskussionen in Deutschland, wozu die Rehabilitation von Homosexuellen, die Pflegesituation, die Kontrolle der Polizei, die Diskriminierung von Frauen z. B. bei Entgeltszahlungen, Transgender, das Kopftuchverbot, viele aktuelle Fragen zur Meinungsfreiheit, das Demonstrationsrecht, vieles mehr und in vielen Beiträgen die Flüchtlingspolitik stehen. Für Beck war dies daher die richtige Plattform für Forderungen zu den Rechten von Flüchtlingen, die nach einer „Kaskade" von Gesetzen zu ihrer „Entrechtung" auf den Schutz der Zivilgesellschaft angewiesen seien.

In 45 Kurzbeiträgen wird knapp und klar auf das jeweiligen Thema eingegangen. Einen gewissen Schwerpunkt bildeten – wieder einmal – Überwachung und Sicherheitsbehörden. Die Reform des bayerischen Polizeigesetzes 2018 ist zwar noch kein Thema, wohl aber die vorangegangene Änderung von 2017, die wesentliche Elemente einer seit Jahren anhaltenden Entwicklung abbildet: die Vorverlagerung von Eingriffsbefugnissen. Die Polizei ist zur Gefahrenabwehr da, die „Gefahr" legitimiert Grundrechtseingriffe. Sie bildet eine Schwelle, die man im Fall Bayerns nun niedriger gesetzt hat: Für viele Maßnahmen soll nun eine „drohende" statt einer „konkreten" Gefahr genügen. Es ist letztlich eine schiefe Ebene hin zu immer mehr polizeilicher Ermächtigung, wie der Beitrag von Anna Katharina Mangold zum „Gefährder" zeigt. Was eine „Gefahr" ist, lässt sich aus Sicht der Wissenschaftlerin noch halbwegs klar umreißen: als eine hinreichende Wahrscheinlichkeit eines bevorstehenden Schadens. Was bei der Einstufung als „Gefährder" maßgeblich ist, sei dagegen reichlich schemenhaft. Sie sei eine Prognose, jemand werde künftig Gefahren schaffen. Da aber die Annahme einer „Gefahr" selbst eine Prognose sei – etwas wird passieren –, laufe der Begriff Gefährder auf die „Prognose einer Prognose" hinaus, also auf dünnes Eis.

Weitere Beiträge handeln von Gesichtserkennung per Video, von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung, also von „intelligenten" Überwachungssystemen. Ihnen ist gemeinsam, dass neue Technik immer tiefer in die persönliche Sphäre eindringen kann. Von einer Videokamera aufgenommen zu werden, ist weitaus harmloser, als automatisiert durch ein Identitätsraster gejagt zu werden. Aber es ist nicht nur die spektakuläre Technik, die an der Freiheit nagt, es sind auch die scheinbar harmlosen Änderungen. Peter Schaar, einst Bundesdatenschutzbeauftragter, wies darauf hin, dass digitale Passbilder neuerdings von Polizei, Nachrichtendiensten und anderen Behörden automatisiert abgerufen werden dürfen. Theoretisch bleibe eine biometrische Zentraldatei zwar verboten, praktisch schaffe die Änderung aber die Voraussetzung dafür, „dass die verteilten Datenbestände der Pass- und Ausweisbehörden online zusammengeschaltet werden können".

Volker Beck erinnerte bei der Präsentation an das Vorratsdaten-Urteil von 2010. Darin mahnte das Bundesverfassungsgericht, das Gesamtbild der Datensammelei in den Blick zu nehmen. „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland" (Janisch, Durchs Raster gejagt, SZ 30./31.05.2018, 6).

Schaffland/Wiltfang
Datenschutz-Grundverordnung (DS-GVO)/ Bundesdatenschutzgesetz (BDSG) – Kommentar, Loseblattwerk, Stand Juli 2018, 2642 Seiten (zwei Ordner), ISBN 978-3-503-17404-1, 118,-- € (Grundwerk, mit Abnahmeverpflichtung der Ergänzungslieferungen für mindestens ein Jahr, 198,--€ ohne Abnahmeverpflichtung)

(wh) Bei Loseblattwerken stellt sich fast immer die Frage: Wann lohnt sich eine Rezension? Dies gilt insbesondere bei Loseblattwerken, die in der ursprünglichen Form schon länger auf dem Markt sind. Dem Rezensionschreiber lag das Werk schon mit dem Stand der Ergänzungslieferung Mai 2018 vor. Zu diesem Zeitpunkt war aber schon klar, dass die in dieser Version noch enthaltene systematische Kommentierung des alten BDSG nur noch von historischem Interesse ist und dass es einige Korrekturen der DSGVO gab, die zu berücksichtigen sein würden. Zudem war das neue BDSG bis dahin im Werk nur bis zum § 26 kommentiert, so dass eine Rezension noch nicht sinnvoll erschien. Mit den Ergänzungslieferungen Juni 2018 und Juli 2018 ist nun die Kommentierung des neuen BDSG vervollständigt worden, mit der Ergänzungslieferung Juli 2018 sind zudem die Korrekturen der DSGVO eingearbeitet und die systematische Kommentierung des BDSG aus dem Loseblatt werk herausgenommen worden: Alles in allem also ein guter Zeitpunkt für eine Rezension.

Bei der Kommentierung der DSGVO im ersten Ordner fällt sofort auf, dass sowohl der Bezug zu den entsprechenden Regelungen des alten BDSG als auch – sofern gegeben – ein Bezug zu entsprechenden Regelungen im neuen BDSG hergestellt wird. Durch diese Gestaltung ist es möglich geworden, die zum alten BDSG erfolgte Rechtsprechung den Regelungen der DSGVO – soweit passend – zuzuordnen. Dies erspart es, ein zweites Werk (z.B. den letzten aktuellen Kommentar zum alten BDSG) bezüglich eventuell anwendbarer bereits vorhandener Rechtsprechung zu konsultieren. Auch wird auf bereits vorliegende Kommentare zur DSGVO anderer AutorInnen verwiesen. Bei neuen Regelungsgegenständen, die im alten BDSG noch nicht enthalten waren, wie z.B. die Anforderungen aus Art. 25 DSGVO, Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen, fällt Kommentierung – verständlicherweise – noch etwas knapp aus.

An vielen Stellen, wie z.B. Art. 28 Auftragserarbeitung oder Art. 32 Sicherheit der Verarbeitung werden neben einer reinen Kommentierung auch hilfreiche weitergehende Hinweise gegeben – so z.B. welche Anforderungen von Aufsichtsbehörden gestellt werden – und in Anhängen Muster vorgelegt.

Auch wenn der zweite Ordner „Bundesdatenschutzgesetz – BDSG“ heißt, lässt die Unterüberschrift „Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften“ bereits erahnen, dass dort nicht nur das BDSG enthalten ist, sondern auch Landesdatenschutzgesetze, das kirchliche Datenschutzrecht der evangelischen und der römisch-katholischen Kirche (das Datenschutzrecht der alt-katholischen Kirche fehlt leider) und diverse bereichspezifische Gesetze. Die Kommentierung beschränkt sich aber – wie vom Titel des zweiten Ordners versprochen – auf das Bundesdatenschutzgesetz. Die Reihenfolge der Landesdatenschutzgesetze und des kirchlichen Datenschutzrechts ist etwas verwirrend. So finden sich zuerst die Landesdatenschutzgesetze der alten Bundesländer (in alphabetischer Reihenfolge), dann zwei kirchliche Datenschutzgesetze und dann die Landesdatenschutzgesetze der neuen Bundesländer (ebenfalls in alphabetischer Reihenfolge). Hier wäre es wünschenswert gewesen, wenn im Rahmen der durch die Novellierungen dieser Regelungen erforderlich gewordenen Aktualisierungen des Werkes die Trennung zwischen alten und neuen Bundesländern aufgehoben worden wäre.

Die Kommentierung des neuen BDSG ist erfreulich ausführlich und um praktische Anwendungsfälle ergänzt. Ebenso wie im ersten Ordner wird hier der Bezug zum alten BDSG hergestellt. Dies gilt insbesondere für die Regelungen des alten BDSG, die für öffentliche Stellen galten.

Alles in allem ist dieses Werk eine sehr umfangreiche und nützliche Kommentierung der DSGVO und des neuen BDSG mit einigen Praxishilfen für die Umsetzung. Wer Loseblattwerke mit Ergänzungslieferungen mag, der/dem kann dieses Werk guten Gewissens empfohlen werden.

Däubler, Wolfgang
Digitalisierung und Arbeitsrecht Internet, Arbeit 4.0 und Crowdwork
6. Aufl. 2018, Bund-Verlag Frankfurt ISBN 978-3-7663-6690-0, 621 S., 29,90 €

(tw) 2001 veröffentlichte der Autor erstmals sein Buch zu arbeitsrechtlichen Fragen, die im Rahmen der Digitalisierung auftreten. Bis zur 5. Auflage aus dem Jahr 2015 trug das Werk noch den Titel „Internet und Arbeitsrecht“. Das wurde nun der Realität angepasst, zumal bei aller elektronischen Vernetzung im Beschäftigungsverhältnis nicht das Internet, sondern die Digitalisierung das zentrale prägende Merkmal ist. Däubler behandelt in dem völlig aktualisierten Werk themenbezogen alle sich um die Digitalisierung rankenden Themen, nicht nur, aber auch den Datenschutz und die Überwachung im Betrieb. Letzteres wird ausführlicher in seinen „Gläsernen Belegschaften“ (DANA 1/2018, 62) behandelt, dazu bestehen natürlich Redundanzen. Die wesentlichen Aspekte werden insofern auch hier abgehandelt und zwar auf aktuellem Niveau mit DSGVO und BDSG-neu. Für Betriebsräte ist das Buch darüber hinausgehend von großem Wert, weil es auch Fragen behandelt, die Beschäftigte beschäftigen, ohne direkt mit Überwachung und Kontrolle zu tun zu haben: Nutzung sozialer Netzwerke, Arbeitszeit, Arbeitsschutz, psychische Belastung, Gewerkschaften, Anspruch auf Qualifizierung, private Nutzung von Geräten, Homeoffice und Mobilnutzung, Internet-Arbeitsverhältnis, Online-Auftragsvermittlung, Crowdwork und IT-Sicherheit. Neben dem individuellen spielt das kollektive Arbeitsrecht eine zentrale Rolle: Mitbestimmungsrecht und Mitbestimmungspflicht beim Einsatz digitaler Technik. In einfacher, klarer Sprache werden die nicht immer unkomplizierten Themen behandelt. Erschlossen sind diese auch über ein ausführliches Stichwortverzeichnis. Adressen, Tipps und eine ausführliches Literaturverzeichnis erhöhen den Nutzen für Betriebsräte, und das alles äußerst preiswert.

Wenn staatliche Hacker mit Bundestrojanern in der Lage sind, Computer und Handys zu durchsuchen, können sie auch Daten kompromittieren.



Wer kontrolliert das?

Gibt es von den Sicherheitsbehörden die Garantie für einen Schutz vor Missbrauch?

Quis custodiet ipsos custodes?

Bild: iStock